

1 Page 1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

DONNA CURLING, ET AL.,

Plaintiffs,

vs. CIVIL ACTION FILE
NO. 1:17-CV-2989-AT

BRAD RAFFENSPERGER, ET AL.,

Defendants.

REMOTE VIDEOTAPED ZOOM DEPOSITION OF
DAVID HAMILTON

January 18, 2022
10:06 A.M.

Lee Ann Barnes, CCR-1852B, RPR, CRR, CRC

Page 2

1 APPEARANCES OF COUNSEL
2 (All appearances via Zoom)
3

4 On behalf of the Plaintiffs:

5 MARY G. KAISER, ESQ.
6 DAVID D. CROSS, ESQ.
7 MORRISON & FOERSTER LLP
8 2100 L Street, NW
9 Suite 900
10 Washington, DC 20037
11 202.887.1500
12 mkaiser@mofo.com
13 dcross@mofo.com

14 - and -
15

16 HALSEY G. KNAPP, JR., ESQ.
17 ADAM M. SPARKS, ESQ.
18 KREVOLIN HORST
19 One Atlantic Center
20 1201 W. Peachtree Street, NW
21 Suite 3250
22 Atlanta, Georgia 30309
23 404.888.9700
24 hknapp@khlawfirm.com
25 sparks@khlawfirm.com

16 On behalf of Secretary of State and the State
17 Election Board:
18

19 CAREY MILLER, ESQ.
20 ROBBINS ALLOY BELINFANTE LITTLEFIELD
21 500 14th Street NW
22 Atlanta, Georgia 30318
23 678.701.9381
24 carey.miller@robbinsfirm.com
25

Page 3

1 APPEARANCES OF COUNSEL
2

3 On behalf of Defendants Fulton County Voter
4 Registration and Elections:

5 CHERYL RINGER, ESQ.
6

OFFICE OF THE FULTON COUNTY ATTORNEY
141 Pryor Street, SW
Suite 4038
Atlanta, Georgia 30303

7

8 Also Present:
9 Marilyn Marks, Coalition for Good Governance
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

Page 4

1 INDEX OF EXAMINATION

2 WITNESS: DAVID HAMILTON

3 EXAMINATION	PAGE
By Ms. Kaiser	9
By Mr. Miller	199

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

Page 5

		INDEX TO EXHIBITS	
	Plaintiffs'		
	Exhibit	Description	Page
1			
2	Exhibit 1	Email Chain, Bates Numbers FORTALICE001200 through -001201	18
3	Exhibit 2	LinkedIn Profile of David Hamilton, No Bates Numbers	22
4	Exhibit 3	Email Chain dated August 2016, Bates Numbers FORTALICE000002952 through -2953	40
5	Exhibit 4	Fortalice Red Team Penetration Test and Cyber Risk Assessment Report for State of Georgia, Office of the Secretary of State, November 2018, Bates Numbers Payton 000070 through -000119	46
6	Exhibit 5	Declaration of David Hamilton, No Bates Numbers	53
7	Exhibit 6	Task order from Fortalice to the Secretary of State's office dated March 11, 2021, Bates Numbers FORTALICE000001 through -2	84
8	Exhibit 7	Weekly Updates from Fortalice to the Secretary of State's Office, Bates Numbers FORTALICE002781 through -2788	65
9	Exhibit 8	Email Chain, Bates Numbers STATE-DEFENDANTS-00126678 through -126682	90
10	Exhibit 9	Email Chain, Bates Numbers STATE-DEFENDANTS-00126696 through -126698	94
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			
21			
22			
23			
24			
25			

Page 6

INDEX TO EXHIBITS		
Plaintiffs' Exhibit	Description	Page
Exhibit 10	News Article, "UPDATE: Ransomware Attackers Hit Hall County Election Infrastructure, dated October 23, 2020, No Bates Numbers	102
Exhibit 11	Email Chain, Bates Number STATE-DEFENDANTS-00104972	104
Exhibit 12	Email Chain, Bates Numbers STATE-DEFENDANTS-00158821 through -158822	109
Exhibit 13	Election Office Notes, 10 AM 6/15/20 Meeting, Bates Numbers STATE-DEFENDANTS-00158823 through -158825	116
Exhibit 14	Email Chain, Bates Numbers STATE-DEFENDANTS-00171971 through -171973	125
Exhibit 15	Email Chain, Bates Numbers FORTALICE001209 through -1212	134
Exhibit 16	Supplemental Declaration of David Hamilton, No Bates Numbers	144
Exhibit 17	Email Chain, Bates Numbers STATE-DEFENDANTS-00126614 through -126616	149
Exhibit 18	Email Chain, Bates Numbers FORTALICE001163 through FORTALICE001166	152
Exhibit 19	Report from Fortalice Solutions dated July 14, 2020, Bates Numbers FORTALICE000625 through -629	158

Page 7

	INDEX TO EXHIBITS		
1	Plaintiffs'		
2	Exhibit	Description	
3		Page	
4	Exhibit 20	Email from David Hamilton dated 4/29/2021, Bates Number STATE-DEFENDANTS-00170625	165
5	Exhibit 21	Email from Dave Hamilton dated 8/21/2020, Bates Number STATE-DEFENDANTS-00161203	172
6	Exhibit 22	Document, Bates Numbers STATE-DEFENDANTS-00161204.xls sx through -161204.xlsx	172
7	Exhibit 23	Document Titled "2020 Security of the Voter Registration System Artifacts and Attestation Pursuant to Rule 590-8-3-.01" dated December 18, 2020, Bates Numbers STATE-DEFENDANTS-00182171 through -00182214	176
8	Exhibit 24	Email Chain, Bates Numbers STATE-DEFENDANTS-00182118 through -182120	179
9		(Original exhibits are attached to the original transcript.)	
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			
21			
22			
23			
24			
25			

1 Deposition of DAVID HAMILTON

2 January 18, 2022

3 (Reporter disclosure made pursuant to

4 Article 8.B of the Rules and Regulations of the
5 Board of Court Reporting of the Judicial
6 Council of Georgia.)

7 VIDEOGRAPHER: We are on the record

8 January 18, 2022, at approximately 10:06 a.m.
9 Eastern time. This will be the videotaped
10 deposition of David Hamilton.

11 Would counsel please identify themselves
12 and who they represent for the record.

13 MS. KAISER: This is Mary Kaiser with
14 Morrison & Foerster on behalf of the Curling
15 plaintiffs. With me today are my colleagues
16 Zach Fuchs, David Cross, and Halsey Knapp.

17 MR. MILLER: This is Carey Miller with the
18 Robbins firm, here on behalf of the State
19 defendants Secretary of State Brad
20 Raffensperger and the State Election Board
21 members.

22 MS. MARKS: This is Marilyn Marks,
23 representative, Coalition for Good Governance.

24 MS. RINGER: Cheryl Ringer, attorney for
25 Fulton County.

1 VIDEOGRAPHER: Would the court reporter
2 please swear in the witness.

3 DAVID HAMILTON, having been first duly sworn,
4 was examined and testified as follows:

5 EXAMINATION

6 BY MS. KAISER:

7 Q. Good morning, Mr. Hamilton.

8 A. Good morning.

9 Q. Can you please state your name and address
10 for the record?

11 A. David Hamilton, [REDACTED]

12 [REDACTED]

13 Q. Thank you.

14 Are you represented by counsel today, sir?

15 A. For the purposes of this proceeding, yes,
16 by Carey Miller.

17 Q. Okay. All right. Have you ever been
18 deposed before?

19 A. Not via video, no.

20 Q. All right. Let me just walk you through a
21 couple of rules of the road, just to -- just to
22 level-set here.

23 So I'm going to be asking you a series of
24 questions. I'll try to make my questions clear, but
25 if you do not hear a question or you don't

Page 10

1 understand it, please ask me to clarify my question.

2 Is that okay?

3 A. Sure.

4 Q. Okay. If you answer, I'm going -- going
5 to assume that you understood the question.

6 A. Understood.

7 Q. We should try not to talk over each other,
8 because the court reporter is going to be taking
9 down everything that we say. So I will try not to
10 interrupt you, and I also ask that you let me finish
11 my question before you begin your answer.

12 Is that okay?

13 A. Certainly. Certainly.

14 Q. Okay. Your counsel may object to some of
15 my questions, but do you understand that unless your
16 attorney instructs you not to answer, that you need
17 to answer all of my questions?

18 A. I do.

19 Q. And you understand that you're under oath
20 today, sir; correct?

21 A. Yes.

22 Q. Is there any reason that you cannot
23 testify truthfully today?

24 A. No.

25 Q. Is there anyone else in the room with you?

Page 11

1 A. No. I'm in my office at home.

2 Q. Okay. And just because we're in a -- in a
3 remote environment, I just want to make sure.

4 Do you have any -- any chat functions or
5 email or anything else open on your computer?

6 A. Just this share for exhibits.

7 Q. The Exhibit Share?

8 A. Yeah.

9 Q. Okay. Okay. Great. Thank you.

10 If you need to take a break at any point,
11 just let me know. I will -- I will just ask that
12 you -- if there's a question pending, if I've asked
13 a question, that you provide an answer to that
14 question before we take a break.

15 A. Sure. That's fine.

16 Q. Thank you.

17 What did you do to prepare for your
18 deposition today, Mr. Hamilton?

19 A. Not an awful lot. I haven't been at the
20 State now for six months. So...

21 Q. Right.

22 When did you leave the State?

23 A. Middle of June of this past year, 2020 --
24 2021.

25 Q. 2021?

Page 12

1 A. Sorry.

2 Q. I think time is a little confused for all
3 of us because of COVID.

4 A. The years, yeah.

5 Q. Right. All right. So thank you.

6 So when did you first learn that we wanted
7 to take your deposition in this case?

8 A. I guess middle of last week.

9 Q. Okay. And how did you learn that?

10 A. I -- we got the -- I got an email from --
11 I'm blanking on it -- Ryan Germany and -- and said
12 that I may get a subpoena. And lo and behold, I
13 did. So...

14 Q. So Mr. Germany reached out to you first
15 about this deposition; is that right?

16 A. Just to let -- let me know that it may be
17 coming.

18 Q. Did you meet with -- with counsel for the
19 State before today in preparation for the
20 deposition?

21 A. Yes, ma'am.

22 MR. MILLER: Objection on relevance.

23 BY MS. KAISER:

24 Q. And when did you do that?

25 A. I guess last week. I can't remember the

Page 13

1 day now, but...

2 Q. Was that just one meeting?

3 A. Yeah.

4 Q. And about how long was it?

5 A. Maybe an hour.

6 Q. Did you review any documents during that
7 meeting?

8 A. Yes.

9 Q. Can you just generally describe what kind
10 of documents you reviewed?

11 A. They were --

12 MR. MILLER: Objection -- David --

13 David --

14 THE WITNESS: Sorry.

15 MR. MILLER: -- I'm going to instruct you
16 not to answer as to documents that were
17 provided by counsel to you.

18 To the extent that, to your knowledge,
19 they are public documents, you can answer the
20 question. But with respect to documents
21 provided by counsel, I'm going to instruct you
22 not to answer.

23 THE WITNESS: Okay.

24 BY MS. KAISER:

25 Q. And, again, I'm just asking generally if

Page 14

1 you could describe the categories of documents that
2 you reviewed.

3 A. They were -- they seemed to be court
4 documents.

5 Q. Did you review any emails?

6 A. I -- I think one of them was a exhibit
7 that had an email in it.

8 Q. Understood.

9 And did you have any other meetings or
10 phone calls or correspondence with -- with the
11 State's counsel regarding the deposition?

12 A. No.

13 MR. MILLER: I'll continue my objection on
14 relevance here.

15 BY MS. KAISER:

16 Q. All right. So it was just the one
17 meeting?

18 COURT REPORTER: If there was an answer, I
19 didn't get it.

20 THE WITNESS: No. Sorry.

21 BY MS. KAISER:

22 Q. And that's a good reminder. Mr. Hamilton,
23 because the court reporter is taking a transcript
24 today, we need a verbal answer, please, to all
25 questions.

Page 15

1 A. Okay. I'm sorry. I probably talked over
2 the end of your question. I'm sorry.

3 Q. No problem. Thank you.

4 Have you spoken with anyone besides
5 counsel for the State about this deposition?

6 A. No. I take that back. Yes, my wife.

7 Q. What did you tell your wife with respect
8 to the deposition?

9 A. Just that I was being deposed for the case
10 that I gave testimony in a couple years ago. So...

11 Q. Okay. Thank you.

12 And I believe you said that the way that
13 you learned about the deposition was receiving an
14 email from Mr. Germany; is that correct?

15 A. Yes, ma'am.

16 Q. And then -- so that was -- was that on a
17 personal email address?

18 A. Same one that you have here, yeah.

19 Q. I'm -- okay. Yeah.

20 Did anybody from the State's -- from the
21 Secretary of State's office or their counsel contact
22 you last year regarding having your deposition taken
23 in this case?

24 A. No.

25 MR. MILLER: Objection. Relevance.

1 BY MS. KAISER:

2 Q. Do you have any idea why the Secretary of
3 State's counsel told us that they were unable to
4 locate you in late 2021?

5 A. I --

6 MR. MILLER: Objection. Relevance. Lack
7 of foundation.

8 BY MS. KAISER:

9 Q. You may answer the question, Mr. Hamilton.

10 A. No, I don't.

11 Q. Do you live at the same home address as
12 when you worked at the Secretary of State's office?

13 A. Yes, ma'am.

14 Q. And did the Secretary of State's office
15 have that address on record, to your knowledge?

16 A. Probably not, because I wasn't an
17 employee.

18 Q. Understood.

19 But they did have your email address; is
20 that correct?

21 A. Yes, ma'am.

22 Q. And so they were able to contact you when
23 they tried?

24 A. I believe so, yes.

25 Q. Thank you.

Page 17

1 Did you receive any notices to retain
2 documents relating to the subject matter of this
3 case at any time?

4 A. No, ma'am.

5 Q. When you were doing work for the Secretary
6 of State's office, you had an email address with the
7 Secretary of State; is that right?

8 A. Yes, ma'am.

9 Q. That was dhamilton@sos.ga.gov; is that
10 correct?

11 A. Correct.

12 Q. Did you use any email addresses other than
13 dhamilton@sos.ga.gov for work that you did for the
14 Georgia Secretary of State's office?

15 A. No. As a practice, we like to keep all of
16 the email on the client's email system. Just keeps
17 things simpler.

18 There might have been some contractual
19 language and things like that that went back to my
20 TrustPoint address. That was
21 david.hamilton@trustpointsolutions.com.

22 Q. Okay.

23 A. That was the firm that I worked for when I
24 was with the Secretary of State.

25 Q. Understood.

Page 18

1 Did you have an email address at -- during
2 the time you worked at the Secretary of State's
3 office, dhamilton@imperialhealth.com?

4 A. That was another client that I had at the
5 same time.

6 Q. And did you conduct any business for the
7 Secretary of State's office using that email
8 address?

9 A. Not on purpose, no.

10 MS. KAISER: Pull up Tab 5, please, Zach.

11 (Plaintiffs' Exhibit 1 was marked for
12 identification.)

13 BY MS. KAISER:

14 Q. Mr. Hamilton, we've loaded an exhibit to
15 the Exhibit Share folder. If you can --

16 A. Okay.

17 Q. -- open that up.

18 MS. KAISER: This will be Exhibit 1.

19 THE WITNESS: It still shows empty right
20 now. I did a refresh.

21 Oh, there it is. Okay. Yeah, I --

22 BY MS. KAISER:

23 Q. This is a -- this is a document that's
24 Bates-marked -- that has a Bates Number
25 FORTALICE001200. And the top email in this chain is

Page 19

1 an email from dhamilton@imperialhealth.com dated
2 July 10, 2020.

3 Do you see that?

4 A. I do.

5 Q. And is that your -- is that your email
6 address?

7 A. It was at Imperial Health down in
8 Louisiana, right. This was a fractional --

9 Q. And --

10 A. -- engagement between the two and I was
11 half-timing it, sometimes in Louisiana, sometimes at
12 the State.

13 Q. Understood.

14 So during the time you were working with
15 the Secretary of State's office, you were also
16 working with Imperial Health; is that right?

17 A. Correct. And other clients as well.

18 Q. Okay. If you look -- if you look through
19 this email chain -- and it starts at the -- it
20 begins at the end, if you will, so the first email
21 is at the bottom.

22 A. Okay.

23 Q. And this looks to be -- the subject of
24 this email chain is "FortaliceSOSGA - Rules of
25 Engagement."

Page 20

1 Do you see that?

2 A. Uh-huh.

3 Q. All right. And there's an email from Paul
4 Brandau at Fortalice Solutions.

5 Do you see that?

6 A. Right.

7 Q. All right. What is Fortalice Solutions?

8 A. Fortalice is a -- is a vendor, a partner,
9 of the State that provides security services, pen
10 testing, pay-as-you-go kind of investigative
11 services on things that are security based.

12 Q. Okay. And Mr. Brandau sent this email to
13 Merritt Beaver, as well as you and some others in
14 the Secretary of State's -- or, sorry, and some
15 others at Fortalice; is that right?

16 A. Correct.

17 Q. And who is Mr. Beaver?

18 A. I'm sorry?

19 Q. Who is Merritt Beaver?

20 A. He's the CIO for the State of Georgia --
21 for the Secretary of State of Georgia.

22 Q. Okay. And then on the first -- first page
23 of the document, you see a response from Mr. Beaver
24 to you and Mr. Brandau.

25 Do you see that?

Page 21

1 A. Yeah, I do.

2 Q. Okay. And so does it appear to you that
3 this document relates to your work for the Secretary
4 of State's office?

5 A. It does.

6 Q. Okay. And your response at the top of the
7 page, where we started, that was sent from your
8 Imperial Health email address; is that correct?

9 A. Right. Just on error --

10 Q. Did you --

11 A. -- because -- because -- because I was
12 probably down there and I didn't change the thing at
13 the top of Outlook.

14 Q. Did you ever collect any emails from your
15 Imperial Health email account for the purposes of
16 this case?

17 A. No, ma'am.

18 Q. Okay. You can put that document aside for
19 now.

20 A. Okay.

21 Q. I'm just going to ask you a few questions
22 about your background, Mr. Hamilton.

23 Where did you get your undergraduate
24 degree?

25 A. I did not go to college.

Q. Oh, okay. Do you have any certifications or -- or professional -- I believe you have some professional certifications; is that correct?

A. I do, yes, ma'am.

Q. Can you tell me about those?

A. I have a CISSP, which is the certification for information security professionals. I have a CISM through ISACA. I have a CDPSE, which is a privacy standard certification. I have a healthcare-specific privacy and compliance certificate and also a certified C|CISO certificate.

Q. That's C-S-E-L?

A. C. and then a bar. C-T-S-O. Right.

Q. Would you say that you have any training in cybersecurity?

A. Yes, ma'am.

Q. How long have you worked in the cybersecurity field?

A. Probably about 15 years now.

MS. KAISER: Pull up Tab 1, please.

BY MS. KAISER:

Q. I'm going to add Exhibit 2 to the Exhibit Share.

A. Okay.

(Plaintiffs' Exhibit 2 was marked for

1 identification.)

2 THE WITNESS: Oops, it logged me out.

3 Hang on a second.

4 BY MS. KAISER:

5 Q. Sure.

6 A. Crap. I'm looking at the wheel. Hang on.
7 It's thinking.

8 Okay. Number 2.

9 Q. Do you recognize this document,
10 Mr. Hamilton?

11 A. Uh-huh. Yes.

12 Q. Is this a copy of your profile from
13 LinkedIn?

14 A. Looks like it.

15 Q. And is this something that you update
16 regularly?

17 A. I haven't in a while. Since -- since I
18 landed at -- at Shepherd, there's not much point in
19 it.

20 Q. Okay. And that was -- when did you begin
21 with Shepherd?

22 A. June, right as I left TrustPoint.

23 Q. In 2021?

24 A. Yes, ma'am.

25 Q. On -- at the bottom of page 1 of this

Page 24

1 document, it indicates that you worked for
2 TrustPoint Solutions from October 2013 to June 2021;
3 is that correct?

4 A. It is.

5 Q. And what is TrustPoint Solutions?

6 A. They're a provider of security and
7 infrastructure services predominantly in healthcare.
8 They have some business outside in the public
9 sector.

10 Q. Sorry. I think you mentioned this, but
11 during the time that you had the title of chief
12 information security officer for the Georgia
13 Secretary of State's office, were you employed by
14 TrustPoint Solutions?

15 A. Yes, ma'am.

16 Q. So did you do work for the Secretary of
17 State's office on a contract basis?

18 A. No, not directly. Always through
19 TrustPoint.

20 Q. So you mean you, yourself, were not under
21 contract; the company --

22 A. Correct.

23 Q. -- TrustPoint was?

24 A. Correct.

25 Q. How much time did you spend per month on

Page 25

1 work at the Secretary of State's office, roughly?

2 A. I guess it averaged out to be probably
3 half-time. There was some spikes there where it was
4 more full time as things ramped up for events such
5 as elections and things, incorporations. End of
6 year was a pretty busy time for the corporation
7 side. But as you look across, I would imagine it
8 would compute to be about half-time.

9 There were some times where I didn't --
10 wasn't there at all during a week because I was at a
11 different client.

12 Q. When you say "there at all," were you
13 physically at the Secretary of State's office?

14 A. Yes, ma'am.

15 Q. And when did you begin working for the
16 Georgia Secretary of State's office?

17 A. Summer of 2018. That's when the
18 engagement first began.

19 Q. And so from roughly summer of 2018 until
20 June of 2021, you spent approximately half your time
21 working on security issues for the Georgia Secretary
22 of State's office; is that correct?

23 A. Yes, ma'am.

24 Q. And what were your responsibilities for
25 the Georgia Secretary of State's office?

1 A. Just overseeing the -- the corporate
2 information security program, which included the --
3 the election side as far -- insofar as it -- the
4 registration side of the house. Not the Dominion
5 side, but the -- the corporation side of the house,
6 which is where you get a business license in
7 Georgia, and then also the Bureau of Licensing,
8 which is all the professional boards, the nursing
9 board and the barbershop folks and all those folks.
10 It's where you kind of go for -- that was the only
11 place that had PHI, so -- protected health
12 information.

13 Q. Understood. Okay.

14 And when you said -- you said that that
15 encompassed the election side insofar as the
16 registration side of the house.

17 Can you explain what you mean by that?

18 A. Well, there's -- there was a couple of
19 different buckets, right? The -- the main
20 things that I was concerned with is the -- is the
21 voter registration, the MVP site; security of the --
22 more or less the public-facing sites that managed
23 the registration of a voter.

24 Didn't have anything to do with the
25 tabulation of votes or the voting machines

1 themselves. All that was handled by the vendor.

2 Q. Interesting. Okay.

3 Who did you report to at the Secretary of
4 State's office?

5 A. Mr. Beaver. Merritt Beaver, the CIO.

6 Q. And did anybody report to you?

7 A. Yes. There was -- we had a couple of --
8 three. At one point there was one, then it got back
9 up to three when we restaffed. There were several
10 names in there. Do you want me to try to recall
11 them?

12 Q. Yes, if you can.

13 A. Okay. When I got there, it was -- I just
14 can't recall his name. Heavyset fella. I can't --
15 probably have to go to LinkedIn to figure that one
16 out. I can't recall his name.

17 When I left --

18 Q. Do you recall -- I'm sorry. Please
19 finish.

20 A. I was just going to say when I left, I can
21 tell you who those folks were.

22 Ronnell Spearman, who is -- who I think is
23 still there; Kevin Fitts; and then there was one
24 person that hired just as I was leaving. I actually
25 never got to meet him in person and I can't recall

1 his name.

2 Q. Do you recall the titles of the -- the
3 people that reported to you?

4 A. Yeah. Just security analyst.

5 Q. As part of your work with the Secretary of
6 State's office, did you work with any outside
7 vendors?

8 A. Yes, ma'am.

9 Q. What vendors were those?

10 A. Probably the largest being Fortalice.

11 They were kind of my right hand, made up for us not
12 having a big staff of folks.

13 Beyond that, we had Dell Secureworks. We
14 had Palo Alto. A lot of the providers of the
15 solutions that we used. Critical Start would be an
16 example. Just -- Clawless [phonetic].

17 Q. And I think you -- you may have mentioned
18 this before, but what services did Fortalice provide
19 for the Secretary of State's office?

20 A. Security services. They did pen testing.
21 You know, we have an annual pen test where we have
22 somebody come in from the outside.

23 And also incident response. So if there
24 was something that came up where we needed some
25 investigative specialty, kind of a subject matter

1 expert on intrusion or one of those guys, they have
2 a bunch of people.

3 They're -- they hired on about the same
4 time that TrustPoint did. We kind of came in about
5 the same time. And we decided to use Fortalice for
6 that half and -- and TrustPoint for the guy that sat
7 in the seat, which was me.

8 It actually started off being Gaylon
9 Stockman, but once things got ramped up, Gaylon left
10 TrustPoint for another job, so it ended up being
11 just me. The idea was to kind of alternate us back
12 and forth to give enough time, but it just didn't
13 work out that way in the end.

14 Q. So originally the job was supposed to be
15 split between two people from TrustPoint --

16 A. Correct.

17 Q. -- TrustPoint?

18 A. Yeah, that was how -- that was how the SOW
19 was written, statement of work.

20 Q. And would that have provided more hours
21 overall of support from TrustPoint, more like a
22 full-time person?

23 A. No, I think the statement of work was
24 still half-time at that point, but the issue was
25 that both Gaylon and I had other commitments that I

Page 30

1 think they were trying to jockey things around and
2 kind of fill the blank spots with the schedules.

3 Q. You mentioned Secureworks as another
4 vendor.

5 A. Uh-huh.

6 Q. What services did Secureworks provide to
7 the Secretary of State's office?

8 A. There's a pretty large contract with
9 Dell -- with Dell Secureworks to provide logging and
10 aggregation of logs and kind of oversight as a -- as
11 a -- you can call it a SIEM, S-I-E-M. It's a
12 security incident event monitoring.

13 And that's -- they kind of watch from
14 afar. They look for patterns. They look for things
15 that happen in -- in the world and then hone in on
16 that.

17 And they're supposed to alert us when
18 things happen, and then we -- we can take action or
19 we can say, "No, that was us" or "That was a test"
20 or things like that.

21 Q. And did they provide services to the
22 Secretary of State's office throughout your tenure
23 there?

24 A. No. We decided to let them go I guess
25 about halfway through my tenure. I think it was

Page 31

1 mostly because I think over time -- they were
2 engaged, I think, long before I got there, but over
3 time, I think the -- the cost kind of crept up over
4 time and it -- it was a very significant investment.
5 So we decided to part company so we could take that
6 money and use it in different ways for different
7 tools.

8 Q. Were you involved in --

9 (Cross-talk.)

10 A. Yes, ma'am.

11 COURT REPORTER: One at a time, please.

12 Were you involved in?

13 THE WITNESS: Sorry. Yes, ma'am.

14 COURT REPORTER: I didn't get the whole
15 question, though.

16 THE WITNESS: Oh, I'm sorry.

17 COURT REPORTER: That's okay.

18 BY MS. KAISER:

19 Q. I said were you -- were you --

20 MS. KAISER: I'm sorry, Ms. Barnes.

21 COURT REPORTER: Go ahead.

22 BY MS. KAISER:

23 Q. The question was were you involved in that
24 decision?

25 A. Yes.

1 Q. As chief information security officer,
2 would you say that you had a relatively senior
3 position in the Secretary of State's office?

4 A. Yeah, as far as a contractor can go. You
5 know, I didn't have any signing authority. I didn't
6 have a budget. I didn't -- you know, it's not like
7 a regular engagement where, you know, there's some
8 distance there.

9 If -- if I was a full-time employee, it
10 would have been a different situation, I think. But
11 I relied on -- on Merritt for a lot of the back
12 office-type operations, and most -- most of my
13 engagement was -- there was basically making
14 recommendations and just -- you know, "I think we
15 should do this," and, you know, Merritt could say
16 yea or nay and we went from there.

17 Q. Do you have a view on whether having a
18 half-time chief information security officer was
19 adequate for an entity the size of the Georgia
20 Secretary of State's office?

21 MR. MILLER: Objection. Lack of
22 foundation. Calls for speculation.

23 THE WITNESS: I can say that I do -- or I
24 did, rather, in the past fractional CISO work
25 for a lot of firms and it worked very well.

1 BY MS. KAISER:

2 Q. And I believe you said you left the
3 Georgia Secretary of State's office in June 2021; is
4 that correct?

5 A. Yes, ma'am.

6 Q. And what were the circumstances for your
7 departure?

8 A. TrustPoint, the company, got acquired by
9 another firm out of Jacksonville, Florida.
10 Optimum HIT is how they pronounce their corporate
11 name.

12 And when they did, they -- they had such a
13 dramatic change in the benefits -- not -- not really
14 compensation, but the benefits side of the house --
15 and it became financially untenable for me to
16 continue, because my wife is disabled and she
17 requires certain medicines and they did not cover
18 them at all.

19 So, basically, my -- my decision to leave
20 was strictly on medical benefits. I mean, I left on
21 good terms. They're still good guys. Work for them
22 again if they could come up with a better health
23 plan. So...

24 Q. Understood. And I'm sorry to hear that
25 about your wife, Mr. Hamilton.

1 So it sounds like this had everything to
2 do with TrustPoint and nothing to do with the
3 Secretary of State's office; is that --

4 A. Oh, sure, no.

5 Q. -- accurate?

6 A. Yeah. Yeah. It was all about -- yeah, I
7 just couldn't -- I couldn't swing it -- I couldn't
8 swing it by myself.

9 And -- and it's interesting that I kind of
10 ended up at a firm that -- that deals with brain
11 injury, which is exactly what my wife had, so they
12 understand my plight, so to speak. So I'm in a good
13 place now.

14 Q. I'm glad to hear that.

15 A. Thank you.

16 Q. I just wanted to circle back to one thing
17 in your background.

18 So I believe you said that when you met
19 with counsel in preparation for your deposition
20 today, you did look at some documents; is that
21 correct?

22 A. Yes, ma'am.

23 Q. And did those documents refresh your
24 recollection about any facts or -- or events that
25 took place pertinent to this case?

1 A. I -- I didn't spend an awful lot of time
2 reading them. We just kind of glazed over them.

3 But, no, I -- I felt pretty good about my
4 memory about things, what happened. So...

5 Q. Did you ever recommend to the Secretary of
6 State at any point that they should have a full-time
7 chief information security officer?

8 A. Yes.

9 Q. Do you recall approximately when you made
10 that recommendation?

11 A. I think, basically, when -- when James
12 Oliver -- he was my predecessor. He was a full-time
13 employee.

14 I think initially when we came in, you
15 know, our edict was to kind of coach him up and get
16 him, you know, kind of more out there.

17 And James, very nice man, but he was kind
18 of reserved and quiet, and it's kind of hard to do
19 this job when you seal yourself in your office. You
20 kind of have to be out there and evangelize security
21 and get people excited about it, and he just didn't
22 have that gene.

23 So I -- you know, when the Secretary of
24 State made the decision to part ways with James, I
25 really thought the next step was for me to help the

1 Secretary of State find another full-time employee.

2 In the end, it wasn't. What they decided
3 to do is do a fractional kind of a situation where
4 they'd continue that relationship and kind of let me
5 sit in the chair.

6 That's not unheard of, but it's -- I mean,
7 I would have rather have them have a full-time
8 employee just for consistency, right? Because you
9 never know if I'm going to get pulled away on
10 another -- on another deal or -- you know. It would
11 have been better, I think, to have a full-time, and
12 I could advise that person kind of as a -- think of
13 it as like a mentor relationship.

14 Q. And I believe you said that you didn't --
15 you personally didn't have a budget.

16 Did you ever make a recommendation that
17 the chief information security officer should have a
18 budget?

19 A. No. I mean, they -- they had a budget for
20 security; it's just I wasn't -- I didn't have any
21 signing authority. I couldn't go spend money. You
22 know, I didn't have an expense account or anything
23 like that.

24 Anything I wanted to spend money on, I had
25 to go to -- go to Merritt for, and he worked it out

1 through back channels.

2 Q. Did you make any other recommendations to
3 the Secretary of State's office regarding security
4 that the Secretary of State did not accept or
5 implement?

6 A. No. I think -- I think most of what we
7 talked about -- you know, we had kind of a list of
8 best practices.

9 We were trying to get them to conform to
10 the NIST standards, the 800-53, which is kind of a
11 very good place to start. And a lot of those things
12 could have been better. You know, if you rated them
13 1 to 5, you had some 1s and 2s. They should have
14 probably been 3s.

15 So over time, I think we picked the
16 low-hanging fruit and fixed the most critical ones,
17 a lot of it just based on judgment, right? You just
18 made a judgment based on what you had and what we
19 could do.

20 I knew there wasn't an unlimited budget
21 for Secretary of State. Like other state agencies,
22 you know, they were -- but I was impressed in the
23 fact that they were able to secure some really good
24 hardware and some really good technologies to be
25 able to kind of build upon, in some cases better

1 than some of my healthcare customers.

2 So, you know, started off -- I guess now
3 Governor Kemp, but Secretary of State Kemp, I think
4 he played a big part in that and funding that and
5 kind of paying attention to the security. It was
6 important to him, and as -- as it was important to
7 Secretary Raffensperger as well.

8 Q. Do you know who has the chief information
9 security officer responsibilities at the Secretary
10 of State's office now, if anyone?

11 A. I don't. I don't. I kind of lost touch
12 with the guys. So...

13 Q. So prior to your departure, you weren't
14 told who was going to step into that role?

15 A. No, they --

16 MR. MILLER: Objection.

17 THE WITNESS: -- they -- I'm sorry.

18 MR. MILLER: You can answer, Mr. Hamilton.

19 THE WITNESS: Okay.

20 They talked about -- I had given Merritt
21 three different kind of recommendations based
22 on my experiences while I was there, and one of
23 them was moving the then service desk manager
24 over to security, because he had passed his
25 CISSP and he was very interested in security,

1 which is awesome -- that's one of the things
2 you need, working in security -- Kevin Fitts.

3 And I think they -- I'm pretty sure they
4 moved him into that group, but it was as a
5 manager, it wasn't as the CISO or the ISO.

6 And there's also a dual role there at
7 Secretary of State, which is the local agency
8 security officer. That's the person that signs
9 off on the ability for people to get background
10 checks, things like that. I believe we turned
11 that over to Ronnell Spearman. He acts in that
12 role. I think we did that right before I left.
13 Because you don't want that seat to go
14 unfilled. Somebody needs to be able to sign
15 those papers. They come through pretty
16 readily. So...

17 BY MS. KAISER:

18 Q. Does that person, the local agency
19 security officer, have any oversight or
20 responsibilities for the election system?

21 A. No. This was -- this was more of an
22 administrative role, where a lot of the -- a lot of
23 the requests we got were from the corporation side
24 of the house and also from the -- the bureau of the
25 licensing.

Page 40

1 It's folks that had the ability to go in
2 and look at people's backgrounds. They wanted to
3 make sure that they were vetted before we allow
4 somebody to look at somebody's personal information.

5 MS. KAISER: Can you add Tab 2, please,

6 Zach?

7 BY MS. KAISER:

8 Q. We're adding a document to the Exhibit
9 Share --

10 A. Okay.

11 Q. -- Mr. Hamilton.

12 (Plaintiffs' Exhibit 3 was marked for
13 identification.)

14 THE WITNESS: Okay.

15 BY MS. KAISER:

16 Q. Do you have Exhibit 3 up?

17 A. I do.

18 Q. All right. This is a document with the
19 Bates Number FORTALICE002952. It's an email chain
20 from August of 2016.

21 Do you see that?

22 A. I do.

23 MR. MILLER: Hey, Mary, can we go off the
24 record just briefly?

25 MS. KAISER: Sure.

Page 41

1 VIDEOGRAPHER: The time is 10:43. We're
2 off the record.

3 (Off the record.)

4 VIDEOGRAPHER: The time is 10:46. We're
5 back on the record.

6 MS. KAISER: So -- so, Carey, I believe
7 you stated a confidentiality objection here.
8 We -- we object to that confidentiality
9 designation of this document. The email at the
10 bottom of the page from Logan Lamb is certainly
11 not confidential, and the email at the top of
12 the page from Merle King has no substance
13 whatsoever. So we don't believe there's any
14 confidential information contained in this
15 document.

16 MR. MILLER: Okay. I -- you know,
17 respectfully, I'm not asking you to waive any
18 rights to challenge the designation, but this
19 was designated by Fortalice. Frankly, I
20 just -- I don't have enough information sitting
21 here today to say otherwise. My concern is
22 purely on the individuals on the Exhibit Share.

23 MS. KAISER: So can you identify any
24 information in the document that you believe is
25 confidential?

Page 42

1 MR. MILLER: No. That -- that's what I
2 just said. It was designated by Fortalice, who
3 I, frankly, would defer to for any sensitive
4 information.

5 MS. KAISER: Okay. You know, I believe
6 this email has been disclosed to the public.

7 But if we're going to insist on it, then,
8 Ms. Marks, we'll ask you to drop off while we
9 discuss this document and we'll let you know
10 when we're finished discussing this -- this
11 document.

12 MR. MILLER: I mean, Mary, I'm willing to,
13 you know, just say -- if it's been disclosed
14 publicly, I trust your -- your judgment there.
15 But I don't want to -- don't imply that I don't
16 trust anybody that's on the call right now; I'm
17 just trying to -- particularly if other
18 documents are coming up, that may be a bigger
19 issue.

20 MS. MARKS: Mary, this is Marilyn. Just
21 let me know what you want me to do.

22 MS. KAISER: Marilyn, you've seen this
23 document before, have you not?

24 MS. MARKS: Yes. In fact, I was the one
25 who first received it in a public records

1 request.

2 MS. KAISER: Okay. So I think -- I think
3 Ms. Marks can stay on for the discussion of
4 this document. It should be brief. And
5 then --

6 MR. MILLER: That's fine by me. I think
7 it's probably more a cue to potentially other
8 documents coming. So I just want to flag it
9 now.

10 MS. KAISER: Okay. Thank you.

11 BY MS. KAISER:

12 Q. All right. Sorry, Mr. Hamilton.

13 A. Oh, no problem.

14 Q. Have you had a chance to review this
15 document?

16 A. I read it, yep.

17 Q. If you look at the email from the -- from
18 Mr. Lamb starting at the bottom of the page on
19 page 1, the second paragraph down, he states, "While
20 attempting to get more background information on the
21 center prior to contacting you, I discovered serious
22 vulnerabilities affecting elections.kennesaw.edu."

23 Do you see that?

24 A. I do.

25 Q. Are you familiar with the situation that's

Page 44

1 being described in this document where Logan Lamb,
2 an independent cybersecurity researcher, identified
3 certain vulnerabilities with this -- with the
4 Kennesaw server, the election server?

5 A. Yeah, I don't really have any recollection
6 of this. This happened before I got to the State.

7 So I know one person on there, Michael
8 Barnes. He was still there when I was at the State.

9 Q. So during your time at the Secretary of
10 State's office, did you learn anything about this
11 incident with Mr. Lamb?

12 A. No. I don't think anybody was named.

13 I know there was a reason that they moved
14 stuff from Kennesaw into the Election Center over in
15 Marietta, but it was just hearsay. I don't have any
16 direct knowledge of it.

17 Q. What was your understanding of why they
18 moved the server from Kennesaw?

19 MR. MILLER: Objection. Lack of
20 foundation.

21 THE WITNESS: I -- I don't know if I could
22 say. I think they just wanted to have it a
23 little more captive and out of the higher ed
24 side of the house. I think it was maybe --
25

Page 45

1 BY MS. KAISER:

2 Q. Did you have any --

3 A. -- the wrong place to put it.

4 Q. Did you have any involvement with making
5 that transition of the Kennesaw server?

6 A. No, ma'am. No, ma'am. That was way
7 prior. 2016, I guess. So...

8 Q. We've mentioned Fortalice several times
9 now.

10 Are you aware that Fortalice conducted a
11 series of cyber risk assessments for the Secretary
12 of State's office in 2017 and 2018?

13 A. Yes, I -- I have knowledge of those.

14 Q. What role, if any, did you have in working
15 with Fortalice on those cyber risk assessments?

16 A. The second one in 2018, I believe that was
17 during my tenure, at least I got the report. The
18 2017, I think they just passed it to me as history.
19 So...

20 Q. And can you tell me, in general terms,
21 what Fortalice found in its 2017 and 2018 cyber risk
22 assessments for the Secretary of State's office?

23 A. There was a number of items. They
24 classified them as high, medium, low, based on their
25 experience, and then gave us an opportunity to

Page 46

1 either accept or -- or deny, you know, what was
2 going on.

3 It gives us a good basis for kind of
4 reprioritizing our work within the State to figure
5 out where we should spend our money and time trying
6 to go after the things that are the most vulnerable.
7 It's a judgment call.

8 MS. KAISER: Can you pull up Tab 3,
9 please.

10 (Plaintiffs' Exhibit 4 was marked for
11 identification.)

12 THE WITNESS: Is there another document?
13 I'm sorry.

14 BY MS. KAISER:

15 Q. It's being loaded right now.

16 A. Okay. I'm sorry.

17 Q. It takes a minute with larger documents,
18 so apologies --

19 A. Gotcha.

20 Q. -- for the delay.

21 A. Okay. Exhibit B. Okay.

22 Q. So if you scroll down to the next page,
23 you'll see this is the cover page of the report.

24 Do you recognize this as the 20- --

25 November 2018 report that Fortalice provided to the

1 Secretary of State's office?

2 A. I think so. Let me go down to the meat of
3 it here. Hang on.

4 MR. MILLER: Mary, this is another sealed
5 document. I can't recall from the 2019 hearing
6 if we -- how we designated this.

7 THE WITNESS: Yeah, this kind of thing
8 should never be made public, but I get it.

9 MR. MILLER: So, Mary, I'll -- I'll ask at
10 this point if we treat it as attorneys' eyes
11 only.

12 And, Ms. Marks, if you could please drop
13 off for the period of time.

14 MS. MARKS: Sure, I will. And if you will
15 let me know when I can safely come back on.

16 | Thank you.

17 (Ms. Marks left the Zoom deposition.)

18 BY MS. KAISER:

19 Q. Mr. Hamilton, have you had a chance to
20 take a look at the document now?

21 A. I have, yep.

22 Q. And do you recognize this as Fortalice's
23 2018 Red Team Penetration Test and Cyber Risk
24 Assessment?

25 A. T do, ven.

Page 48

1 Q. If you could turn to page 8 of the report.

2 A. Okay.

3 Q. The top section there says " [REDACTED]

[REDACTED] "

5 Do you see that?

6 A. Correct.

7 Q. That next paragraph reads, " [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] "

11 A. Right.

12 Q. If you skip one sentence, it says, " [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] "

17 Do you see that?

18 A. I do.

19 Q. So do you understand this section of the
20 report to address progress made on the top ten risks
21 identified by Fortalice in 2017?

22 A. Uh-huh. Yes.

23 Q. Do you know why three of those top ten
24 risks were not tested in 2018?

25 A. I do not. Usually, it's a -- when a --

Page 49

1 when a security firm does a -- a pen test or a
2 security assessment, they use last year and the
3 current year to show progress or show kind of a
4 trend, are you getting better or are you getting
5 worse. So usually you test the same things.

6 The only reason I would think that we
7 missed is if they were specifically taken out of
8 scope.

9 Q. Okay. And this report says that of the
10 top ten risks identified in 2017, only three had
11 been remediated in 2018; is that correct?

12 A. That's what this states, correct.

13 Q. If you can flip to page 5 of the report.

14 A. Okay. Hang on. It's back. Hang on.

15 Okie-doke. I'm here.

16 Q. The second paragraph on page 5, it reads,

17 " [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED] . "

22 Do you see that?

23 A. Right.

24 Q. And that first bullet point reads, " [REDACTED]
[REDACTED] "

1 Do you see that?

2 A. I do.

3 Q. And are those recommendations detailed on
4 pages 6 and 7 of the report --

5 A. I believe so.

6 Q. -- in this table?

7 A. Yeah.

8 Q. What steps did the Georgia Secretary of
9 State's office take to implement these 20
10 recommendations from Fortalice?

11 A. I can't speak to the first half of that
12 year because I wasn't there, but it might have had
13 something to do with -- and this is a little bit of
14 speculation on my part -- is that that might have
15 been the reason for our involvement, is that Merritt
16 didn't feel like things were moving along fast
17 enough.

18 So he wanted -- that was one of the things
19 that we were to come in and coach up for James
20 Oliver is to kind of get him excited about this
21 stuff and get moving on some of these things that
22 were identified.

23 And I think this was the list that I gave
24 the status on I guess about halfway through the
25 tenure. That was one of the exhibits or the

Page 51

1 statements that I made to the Court.

2 So I don't know what the status is now, of
3 course, because I've been gone six months, but they
4 were well on their way to taking care of those
5 and -- and others that were found along the way.

6 So...

7 Security is -- itself truly is a -- it's a
8 journey; it's not a destination. You're never done.
9 I mean, there's always -- the threat landscape
10 changes every day. Things change every day.

11 So, you know, it's a snapshot in time. At
12 the time that Fortalice did this, this is what they
13 found. They could have waited three weeks and did
14 another one and found something else and not found
15 three others. So it's just a snapshot in time.

16 Q. Sure.

17 At the bottom of page 5 of the report, the
18 last paragraph there, it says, " [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]."

23 Do you see that?

24 A. I do.

25 Q. To your knowledge, did the Secretary of

Page 52

1 State's office dedicate any additional resources to
2 addressing the security risks Fortalice identified?

3 MR. MILLER: Objection. Lack of
4 foundation.

5 THE WITNESS: I believe I was one of those
6 resources.

7 BY MS. KAISER:

8 Q. Do you have any awareness of whether
9 internally at the Secretary of State's office, any
10 additional resources were applied to addressing
11 these security risks?

12 A. Yeah, when -- I was able to recall that
13 gentleman's name, Adam Abell. He -- he was the one
14 that was working with James on a day-to-day basis.
15 So it was only the two of them.

16 Shortly after my arrival, they moved
17 Ronnell Spearman over from the services side of the
18 house and opened up a req for adding another party
19 to the security. I think all of that was based on
20 the findings.

21 So most of the time that I was there, we
22 were at a staff of three and -- not including me,
23 except when we ended up letting one guy go and that
24 gap of time when we were looking for the next
25 person.

Page 53

1 MS. KAISER: Will you add Tab 4, please,
2 Zach.

3 BY MS. KAISER:

4 Q. We're going to bring up the next exhibit,
5 Mr. Hamilton.

6 A. Okay.

7 (Plaintiffs' Exhibit 5 was marked for
8 identification.)

9 BY MS. KAISER:

10 Q. If you scroll down to the second page, I
11 believe you -- you stated that you -- you know, you
12 made a statement in this case.

13 Do you recognize this to be the
14 declaration that you provided in this case?

15 A. Yes, ma'am. One of two, correct.

16 Q. Correct.

17 Let's see. This one is dated August --
18 August 25, 2020.

19 Do you see that?

20 A. That sounds about right, yep.

21 Q. Okay. Did you draft this document, sir?

22 A. I did.

23 Q. And the purpose of your declaration, as
24 you mentioned, was to go through the recommendations
25 from Fortalice and give a status update on how they

1 were being resolved or remediated; is that right?

2 A. Correct.

3 Q. I just want to walk through a couple of
4 these.

5 So Number 2, the "Two-Factor
6 Authentication," do you see that?

7 A. Uh-huh.

8 Q. It says the "Status" was "Accepted and
9 Partially Remediated."

10 A. Uh-huh.

11 Q. Do you see that?

12 All right. And Number 5 was "Non-Unique
13 Local Admin Passwords."

14 Do you see that?

15 A. I do.

16 Q. The "Status" was "Accepted and
17 Compensating Control Applied."

18 Do you see that?

19 A. Correct.

20 Q. What did you mean by "compensating control
21 applied"?

22 A. The long-term solution would be to go to a
23 PAM, which is a privileged account management
24 solution, but that's a pretty heavy lift
25 financially.

1 So in the short term, what we did is apply
2 the out-of-the-box LAP Solution that allows the --
3 the encryption of the endpoints.

4 And also we put in some policy and
5 procedures that when the guys were out working on
6 people's machines, that they -- they have to go to a
7 centralized password vault to be able to access
8 them.

9 They -- in the past, they had the same
10 administrative password on all the systems to make
11 it easy to maintain, you know, your IT help desk
12 guys. But it was a problem for me because I -- I
13 knew that, you know, there was some churn in that,
14 and it's just not a best practice. You should have
15 a unique admin password on every endpoint.

16 Q. Number 10 is "Lack of Security Controls
17 for PCC."

18 You see that?

19 A. Right.

20 Q. And the "Status" for that is "Accepted and
21 Remediation On-Going."

22 A. Yeah. I -- I -- during my tenure there at
23 the State, I think that was the most difficult
24 vendor to deal with, the PCC folks, because they
25 would say one thing and do another.

1 And I even got to the point where I sent
2 them an attestation of a -- basically, a list of
3 minimum security. I just wanted somebody to sign
4 their name to the fact that, you know, some -- the
5 minimum is being done. And they signed it, but in
6 my heart of hearts, I kind of knew that they
7 probably weren't doing it.

8 So -- but at that point, they had already
9 made the decision to remove PCC and move to another
10 vendor, so it would have been kind of wasted breath
11 at that point. Which was, I -- I think, a good -- a
12 good decision to move away from PCC. They just --
13 they just weren't the right guys. That's all.

14 Q. And we'll come back to PCC later on
15 today --

16 A. Okay. Okay.

17 Q. -- but just quickly, what did they have
18 responsibility for with respect to the election
19 system?

20 A. The coding, the actual coding of the
21 program itself. The Secretary of State didn't
22 employ anybody that -- that actually wrote computer
23 code, that developed applications. They -- they
24 always relied on third-party vendors for that.

25 And they did the ENET system and they did,

1 you know, the corporation side and -- and also some
2 of the licensing sites as well. They were kind of
3 the go-to company for all things Secretary of State.

4 I think prior to my arrival, the word
5 was -- is they were a lot better back then. But
6 they had some changes. A lot of people left, good
7 people left, that kind of thing, and over time it
8 just became a problem. So...

9 Q. A problem from a security perspective, was
10 that your view?

11 A. Yeah. Even -- yeah, even the stability of
12 the code line, I think, was wearing very, very thin
13 on the customer, being the Secretary of State. They
14 were getting tired of, you know, things that -- you
15 had mentioned before the confidential --
16 confidentiality, integrity, and availability. That
17 availability part of that triad is pretty important
18 when it comes to the Secretary of State. They
19 always want to be available because they don't want
20 to be viewed as, you know, not on the -- not on the
21 ball.

22 So -- and there were some availability
23 problems with PCC. Some of their practices were not
24 best -- best practice. And they would fix things on
25 the fly and although it fixed it at the moment, they

Page 58

1 wouldn't move that fix back into the code line, so
2 the very next time they did a revision, they would
3 re-break the thing.

4 And that is kind of a, you know, 101
5 change control operation. Somebody wasn't watching
6 the store. So...

7 And we tried to help grow them. You know,
8 we gave them a lot of feedback, probably a lot more
9 than they ever wanted.

10 And then they were purchased by another
11 firm, and that gentleman -- they had a CISO there.
12 He's the gentleman that actually attested to the
13 fact that their minimum security met the minimum
14 based on what I had sent them. I think he was
15 hopeful that it would get that way, but I had my --
16 like I said, I had my doubts, so to speak.

17 Q. All right. Well, going back to your
18 declaration, Mr. Hamilton, we can -- we can keep
19 walking through them one by one, but by my count,
20 there were 11 out of 20 recommendations that,
21 according to your declaration, had not been fully
22 remediated.

23 A. Right.

24 Q. Does that sound about right?

25 A. (Nodded head.)

1 Q. Okay. And that was the status as of
2 August 2020; correct?

3 A. Correct, so basically three months into my
4 tenure. That's about right, yeah.

5 Q. Three months into your tenure. Okay.

6 And -- but that was nearly two years after
7 Fortalice issued their cyber risk assessment in
8 November 2018; is that correct?

9 A. Correct.

10 MR. MILLER: Objection. Lack of
11 foundation.

12 BY MS. KAISER:

13 Q. And so nearly two years after Fortalice
14 issued that report, at least half of their
15 recommendations had not been fully implemented; is
16 that correct?

17 MR. MILLER: Objection. Asked and
18 answered.

19 THE WITNESS: It sounds like it, yeah.

20 BY MS. KAISER:

21 Q. Based on your experience and training,
22 does it seem reasonable to have a cybersecurity
23 vendor identify security risks in your system and
24 then not take recommended steps to address those
25 risks for nearly two years?

Page 60

1 MR. MILLER: Objection to form. Lack of
2 foundation. Calls for speculation.

3 THE WITNESS: In -- in my professional
4 opinion, it's not uncommon. Some of -- some of
5 the things that we're faced with have budgetary
6 constraints.

7 The bottom line is we present -- as
8 security people, we present to the business and
9 say, "Here's the nine things we've got to do.
10 You know, what's our bucket of money look like?
11 What does it take, you know, horsepower,
12 people, whatever?" And then the business makes
13 the decision finally on -- on what -- what to
14 focus on. We make recommendations and then we
15 move on those.

16 But we made pretty good headway, I
17 think --

18 BY MS. KAISER:

19 Q. Were you pushing the Secretary of
20 State's --

21 A. -- before I left. So...

22 Q. Were you pushing the Secretary of State's
23 office to move faster or make more headway on these
24 recommendations from Fortalice?

25 A. Yes, ma'am. I was kind of the evangelist,

Page 61

1 and, yeah, I was -- I was not shy about it. So...

2 Q. Why were you pushing that?

3 A. Just to get -- get moving, right? We had
4 the time and some of the things, like was outlined,
5 are low cost or no cost. It doesn't mean that it --
6 I mean, no cost is nobody has to write a check to a
7 vendor.

8 But the big thing is -- is the headcount.

9 It's the talent that you have in-house that are able
10 to do these tasks. And a lot of my time there
11 was -- was training, mentoring, kind of teaching
12 people how to kind of ramp things up. So -- yep.

13 Q. Have you -- you felt that these
14 recommendations from Fortalice were good ones,
15 correct, that would improve the security of the
16 system?

17 A. Yeah. That's why on -- on the -- on the
18 statement where I said "Accepted" -- in any -- in
19 any situation where a -- a security firm comes in
20 and does an assessment or a pen test and they
21 present you with the findings, you're able to accept
22 those or not accept them.

23 An example of not accepting is either it
24 was out of scope or something that had long been
25 fixed and they missed it. You know, things like

1 that.

2 So in most of these cases, I believe I
3 accepted most of these because I verified that they
4 were still valid.

5 Q. Has Fortalice done any additional work for
6 the Secretary of State's office since the
7 penetration testing in 2018?

8 A. I -- I -- they had an annual -- they had
9 an annual test and assessment, a pen test.

10 Q. And when you say "pen test" --

11 A. I know we --

12 Q. -- is that --

13 A. Penetration test. That's somebody from
14 the outside tries to get in. There's three forms of
15 that. There's, you know, the white hat, the black
16 hat, and the gray hat.

17 So this was very much -- we did not give
18 them the keys to the castle. We wanted them to
19 replicate the outside world, so that becomes a black
20 hat operation.

21 Gray hat is when you give them a little
22 bit of a path, you know a little bit about the
23 environment.

24 And then white hat, of course, is you give
25 them carte blanche to the environment and then they

1 just go -- usually that's an internal pen test.

2 But all of these were external.

3 Q. And to your understanding, Fortalice did
4 one of these pen test assessments each year since --

5 A. Yes, ma'am.

6 Q. -- 2018?

7 And did they test the -- the entire part
8 of the Secretary of State's network or -- or
9 portions of it in those years, do you know?

10 A. Most of it was just the business network,
11 right? It was the business network and the
12 public-facing websites, nothing specific to --

13 You know, every business has a certain
14 number of IP addresses that face the public, and I
15 think in previous years, because of cost, they had
16 kind of truncated that list a little bit. Because
17 they do charge per IP address.

18 And I know one of the years that I was
19 there, I went ahead and had them test everything,
20 every public IP address that we had. It was
21 expensive to do, but you -- you kind of want a basis
22 to kind of run from. So...

23 Q. Did these pen -- penetration tests include
24 the portions of the election system that the
25 Secretary of State is responsible for?

1 A. Yes, ma'am. The registration side, yes.

2 Q. Did you personally work with Fortalice on
3 these penetration tests?

4 A. No. I -- I'm just the client. They're
5 done in a vacuum and then they report back in a
6 draft mode and we talk about them, and then they
7 make a final report.

8 Q. Did they provide those reports to --

9 A. To Merritt, yeah. Again --

10 Q. Did you review --

11 A. -- that was done because they were the
12 customer.

13 Q. Correct.

14 But did you review those reports?

15 A. I did.

16 Q. And you said that there were discussions
17 of the reports.

18 Were you involved in the discussions?

19 A. I would say most of them, but maybe not
20 all of them.

21 Q. So to your knowledge, Fortalice conducted
22 and provided a report regarding a penetration test
23 in 2019; is that correct?

24 A. I would think so, yes.

25 Q. And in 2020?

1 A. I'm not sure because of the COVID stuff.
2 I don't know if that happened.

3 Q. And how about 2021?

4 A. Again, I don't know.

5 MS. KAISER: Can you mark Tab 6, please?

6 I'm sorry, Tab 7.

7 BY MS. KAISER:

8 Q. We're adding two documents to your folder,
9 Mr. Hamilton. I'd actually like to start with the
10 second one.

11 A. Okay.

12 MS. KAISER: 7; is that right?

13 (Plaintiffs' Exhibit 7 was marked for
14 identification.)

15 BY MS. KAISER:

16 Q. Exhibit 7.

17 A. Okay.

18 Q. Do you recognize this document?

19 A. Something I guess from Fortalice. I --
20 we -- we didn't have Microsoft Teams then. I guess
21 that would be a Fortalice thing.

22 Q. Yeah, that was one of my questions. It
23 says -- at the top of this page, it says, "This page
24 is automatically updated from the Wiki in Microsoft
25 Teams."

1 Did --

2 A. Yeah.

3 Q. Do you know what a "Wiki" is?

4 A. Yeah. It's a -- just a database of
5 information.

6 Q. Do you know whether the Secretary of
7 State's office maintained a Wiki with Fortalice
8 through Microsoft Teams?

9 A. No, ma'am. Not -- not to my knowledge.

10 Q. So this isn't something that you've seen
11 before?

12 A. No, ma'am.

13 Q. It looks to be weekly updates from
14 Fortalice to the Secretary of State's office
15 starting in September 2020 and going through
16 July 2021.

17 A. Right.

18 MR. MILLER: Objection. Lack of
19 foundation.

20 BY MS. KAISER:

21 Q. Do you have any reason to believe that's
22 not what this document represents?

23 A. No. I think that -- that's probably what
24 it is. We might have -- we might have gotten these
25 updates via email.

Page 67

1 Q. If you look at the entry for December --
2 excuse me -- yeah, December 4, 2020, I think it's on
3 page --

4 A. Oh, hang on. I went the wrong way. Hang
5 on.

6 Oh, I got --

7 Q. On the --

8 A. Sorry. I go from 6/11 to 6/18. Which --
9 which date? Sorry.

10 Q. This is December 4, 2020. It's on the --

11 A. December. Okay.

12 Q. -- page ending in -2786 at the bottom.

13 A. December 18. Okay.

14 Q. I'm sorry. December 4th, which is a
15 little bit -- just a little bit further down on that
16 same page.

17 A. December 4. Gotcha. Okay.

18 Q. Do you see under "Project Status," the
19 second bullet there says, "Pen test aiming for
20 Feb/March 2021"?

21 A. Right.

22 Q. Does that indicate to you that Fortalice
23 was planning to do penetration testing for the
24 Secretary of State's office in 2021?

25 A. Sounds like it.

1 MR. MILLER: Objection. Lack of
2 foundation.

3 BY MS. KAISER:

4 Q. Let's see. If you move forward on this
5 document to the February 26, 2021, entry.

6 A. Okay.

7 Q. It's on the page ending in -2785.

8 A. -2785. Okay. I got it.

9 Q. The last bullet there says, "Weekly
10 update." It says, "vCISO services have been
11 mentioned."

12 A. Right.

13 Q. "Kyle and Paul are setting up meeting to
14 discuss with Dave Hamilton to get them caught up on
15 a backlog of security tasks."

16 Do you --

17 A. Right.

18 Q. -- see that?

19 A. Right.

20 Q. Do you know what that is referring to?

21 A. Yeah. I had mentioned to Fortalice that I
22 was planning on leaving the State as soon as I found
23 another position and that they needed to -- you
24 know, as the other partner, if they had the ability
25 to step in.

1 You know, I wanted to take care of the
2 State. TrustPoint did not have any resources they
3 had left, so there wasn't anybody from our firm.
4 And I checked it out with my boss and he said it
5 would be fine to kick it to them and say, "Listen,
6 you know, we want to take care of our customer and
7 if you're getting ready to leave, then, you know,
8 you need to give it to them."

9 They subsequently decided that they
10 couldn't fill that seat because of a conflict of
11 interest.

12 Q. What was the backlog of security tasks
13 that are --

14 A. I think --

15 Q. -- mentioned here?

16 A. I think I pitched to them that there was
17 definitely work to be done, it was a work in
18 progress, and it wasn't going to be -- I think my
19 emphasis there was for -- for them to please be
20 interested, you know.

21 Because they would want to bill,
22 obviously. They didn't want to just come in and be
23 a -- more of a maintainer than a fixer, right? So
24 my emphasis there was just to kind of get them
25 interested in coming in and stepping in for me.

1 Q. In your view, why was there a backlog of
2 security tasks?

3 A. Well, I think it was just, you know, we
4 needed some help. You know, we had some staff
5 turnover and some people leave and I was getting
6 spread pretty thin between there and Imperial and I
7 wasn't there every week, and I just felt like I
8 needed to kind of get people interested in coming to
9 help.

10 Q. If you move forward in the document to the
11 entry for April 16, 2023 [sic], it's on the page
12 ending in -2784.

13 A. -2784. Okay. April 16 you said?

14 Q. 16, yes.

15 A. Yes, ma'am. Got it.

16 Q. It says "Project Status," and the second
17 bullet point there says, "Pen test wrapping up."

18 Do you see that?

19 A. Okay. Adam Brown. Okay.

20 Yeah, I worked with --

21 Q. Does that suggest --

22 A. -- Adam.

23 Q. Does that suggest to you that Fortalice
24 did conduct penetration testing in 12 --

25 A. Sounds like it, yeah.

1 COURT REPORTER: Whoa, whoa, whoa, whoa.

2 Excuse me. Can you repeat your question,
3 please?

4 MS. KAISER: Sorry.

5 BY MS. KAISER:

6 Q. The question was, does that suggest to you
7 that Fortalice did conduct penetration testing in
8 April of 2021?

9 A. And I said, yeah, it does sound like it.

10 Q. And if you move forward to April 30, 2021.
11 It's the first entry -- or, sorry, the last entry on
12 the next page, -2783.

13 You see that?

14 A. Okay. "Pen test draft...out." Right.

15 Q. Yep. "Pen test draft...out," yep.

16 So does that suggest to you that Fortalice
17 provided a draft report regarding the penetration
18 testing in 2021?

19 A. Sounds like it --

20 MR. MILLER: Objection --

21 THE WITNESS: -- yeah.

22 MR. MILLER: -- lack of foundation.

23 COURT REPORTER: Repeat the objection,
24 please.

25 MR. MILLER: Lack of foundation.

1 COURT REPORTER: Thank you.

2 BY MS. KAISER:

3 Q. If you go up to the first entry in the
4 document for July 15, 2021.

5 Do you see that?

The last bullet point there under "Weekly Update," it says, "Red team establishing assumed breach."

9 | Do you see that?

10 A. What -- I'm sorry. Which page are we on
11 again? I got lost.

12 Q. Sorry. We're on the first page of the
13 document.

14 A. Oh, sorry. Okay.

15 | Yep, I got it.

16 Q. What does, "Red team establishing assumed
17 breach" mean?

18 A. There's a couple of different ways to
19 approach a client when you're doing red team
20 exercises. And I wanted -- I wanted them to -- or
21 somebody -- probably was me -- wanted them to act
22 like, you know, we had a breach and we needed to
23 also exercise the incident response plan as part of
24 the red team exercise.

25 Q. What is the incident response plan?

1 A. It's a set of documentation, policies,
2 procedures that tells people what their roles are.
3 There's certain people that are identified in the
4 organization that kind of -- think of it like
5 everybody heads to the war room and chats about it.

6 When -- when the security team has an
7 event, that event then -- with further kind of
8 research, if it seems like it is a security issue,
9 then we refer to it as an incident.

10 It is not the security team's privy to
11 deem something as a breach. We can only show it as
12 a potential breach, and then it's up to management
13 to make that decision whether something is actually
14 a breach. We just -- we just give the facts to
15 leadership and they make the determination whether
16 something's a breach or not.

17 Only the senior leadership team can
18 implement the incident response plan and kind of
19 move forward with that.

20 Q. Who is on the -- that management team?

21 A. Legal -- by name or title? I'm sorry.

22 Q. Either.

23 A. Okay. So it would be somebody from legal,
24 somebody from public relations, somebody -- usually
25 two or three people from the senior leadership team,

1 somebody from operations, service desk. Anybody
2 involved directly in the incident gets drafted into
3 that meeting.

4 It's just basically to get all the facts
5 out on the table. You whiteboard everything and
6 then you -- there's a playbook that we kind of go by
7 to certify something as real. We score it based
8 on -- it's a judgment, right? We score it based on
9 criticality, and that's how that kind of runs
10 through that program.

11 Q. And were you part of that management team?

12 A. I was as the -- as the CISO, yes.

13 Q. Do you recall what they -- what the
14 results or findings were from Fortalice's 2021
15 penetration testing?

16 A. Not -- not by heart. Sorry.

17 Q. Do you recall anything generally?

18 A. I think it was just a continuation of
19 the -- you know, the path that they were on. I
20 think they found some new things, I think there were
21 some things from the old report, and then there was
22 things that we fixed. So just part of that journey
23 that I mentioned.

24 Q. Do you recall whether Fortalice sent a
25 final version of their report from this penetration

1 testing?

2 A. Yeah, all those would have been uploaded
3 to a -- a document site, and that, I believe, Ryan
4 and Merritt had access to. Because usually when I
5 got the report, it was from one of those two guys.

6 Q. So to your knowledge, there was a
7 document -- like a document share site for
8 Fortalice --

9 A. Uh-huh.

10 Q. -- in the Secretary of State's office?

11 A. Yes. Yeah, I had an account there to be
12 able to upload things as artifacts, things that I
13 found, stuff like that.

14 Q. Did that have a name?

15 A. It was a commercial site. I -- it's -- I
16 don't want to say -- it wasn't like a Box or a -- it
17 might -- might have been like a share file type.

18 Q. Okay.

19 A. Based on what I remember about Fortalice,
20 it was probably locally held. It probably wasn't a
21 cloud service, because they were a little paranoid
22 about that. So I would say that it was something
23 that they owned in their own private space.

24 Q. All right. Mr. Hamilton, I have a few
25 more questions about Fortalice, but I know we've

1 been going about an hour and a half. Would you like
2 to take a short break?

3 A. I'm okay. I've got my Diet Coke. Keep on
4 going.

5 Q. Okay. Glad to hear it.

6 All right. So let's go back to --

7 (Off-the-record discussion.)

8 BY MS. KAISER:

9 Q. Can you look back at Exhibit 1, please?

10 A. Okay.

11 MR. MILLER: And, Mary, I haven't been
12 looking at the participant list, but if
13 somebody wants to email Ms. Marks if we're done
14 with that section.

15 MS. KAISER: We are, although this
16 document is also marked "AEO" by Fortalice.
17 So --

18 MR. MILLER: I think that's the one we
19 came to the conclusion on earlier, right --

20 MS. KAISER: Oh, no.

21 MR. MILLER: -- Exhibit 1?

22 MS. KAISER: No. I'm sorry. It was a
23 different one.

24 MR. MILLER: Oh, I thought you said
25 Exhibit 1. I apologize.

1 MS. KAISER: We're looking at Exhibit 1.

2 I think it was Exhibit -- it was the Logan Lamb
3 email that was decided --

4 MR. MILLER: Yeah, you're right. You're
5 right. I'm sorry. Okay.

6 BY MS. KAISER:

7 Q. All right. Mr. Hamilton, so do you
8 recognize this document as an email chain from
9 July 2020?

10 A. Yes, yes.

11 Q. And, see, the first email came from Paul
12 Brandau at Fortalice; is that right?

13 A. Correct.

14 Q. Who is Mr. Brandau?

15 A. He was an employee of Fortalice at the
16 time. I think he left shortly after this
17 engagement, but I'm -- I'm not for sure on that.

18 Q. And what was this engagement? What do you
19 recall this engagement was?

20 A. This would have been some -- this was
21 probably pen test from the outside.

22 Q. So in -- in the first email in the chain,
23 Mr. Brandau sent this to Merritt Beaver and to you
24 and two others at Fortalice. He said, "Sending
25 along here to cover down on all aspects - Rules of

1 Engagement included."

2 Do you see that?

3 A. Right.

4 Q. What are the "Rules of Engagement"?

5 A. It's a formal document that usually any
6 kind of pen tester will give a client that -- you
7 can liken it to a "get out of jail free" card.

8 Because, basically, attacking any website,
9 public or -- it's against the law in -- in a lot of
10 states. There's been a lot of media coverage on
11 guys that end up in the pokey because they had a
12 real job and they were trying to do the right thing.

13 So the Rules of Engagement is basically a
14 document that outlines, "Here's what we're going to
15 do; here's what we're going to try to attack; here's
16 the time frame that we're going to do it within."

17 And they do that for two reasons. They
18 give us the time frame so we can not implement the
19 incident response plan thinking it's a real -- a
20 real person, we kind of know they're doing it.

21 So -- and the pretext there is just to
22 kind of give them a paper trail of saying that,
23 "Hey, we discussed this fully with the client and
24 they knew what was happening," and they can't come
25 back later and say, "Oh, you bad people. You

1 shouldn't have done what you did." So that's
2 basically it.

3 Q. The next email, Mr. Beaver responded and
4 said, "Dave, please take ownership of this and get
5 them started."

6 Do you see that?

7 A. Right. Right. Yeah.

8 Q. So you were tasked with overseeing this
9 penetration testing?

10 A. Right. And I think the reason he did that
11 is because I didn't have any signatory -- you know,
12 I couldn't sign the statement of work. I
13 couldn't -- you know, I wasn't given that. So
14 that's probably why Merritt got passed that.

15 Q. Okay. And the next sentence says, "We
16 need to get a good understanding of any
17 vulnerabilities of OLVR and MVP."

18 A. Right.

19 Q. Do you see that?

20 A. Right.

21 Q. What does "OLVR" stand for?

22 A. Online voter registration, and MVP is My
23 Voter Page.

24 Q. So these are -- these are components of
25 the voting system; is that right?

Page 80

1 A. Registration, right. Public-facing web
2 base.

3 Q. Why did the Secretary of State's office
4 think that there may be vulnerabilities with OLVR
5 and MVP at this time?

6 MR. MILLER: Objection. Misstates
7 testimony not in evidence.

8 THE WITNESS: Yeah, I'm -- I'm not really
9 sure that they did. It's just a common thing
10 that we test every year, regardless of what's
11 happening. We want to be --

12 BY MS. KAISER:

13 Q. You wouldn't have any --

14 A. -- in front of the bad guys, right? So we
15 test.

16 Q. Were OLVR and MVP part of the penetration
17 testing that Fortalice conducted each year, to your
18 knowledge?

19 A. I believe so, because they were perimeter
20 websites. So -- especially the one where I opened
21 it up and had them hit all the publics. So yeah.

22 Q. So do you have any understanding of why
23 Mr. Beaver specifically called out OLVR and MVP in
24 this email if they were part of the penetration
25 testing each year?

Page 81

1 A. No. I -- he was just probably telling me
2 to get busy.

3 Q. Was it important to understand any
4 vulnerabilities with OLVR and MVP?

5 A. Always, right.

6 Q. And why is that?

7 A. Well, it's just a very visible system, a
8 lot of -- a lot of stuff going on.

9 You know, we had a lot of public interest
10 in it, a lot of media attention. I'm sure that
11 drove part of his understanding of why we were
12 interested in it. That way we'd have the answers
13 before somebody asked.

14 Q. What work did Fortalice do to assess any
15 such vulnerabilities with OLVR and MVP in 2020?

16 A. I -- I don't specifically know what tools
17 they used. I mean, they're widely -- there's a
18 bunch of different kind of tools, but -- some of
19 them are automated, some of them are manual.

20 They run, basically, robots against all
21 the outside sites, look for certain vulnerabilities,
22 open ports, things that might -- you know, might
23 have not been caught in a previous test.

24 And then, you know, it gives them a list
25 of what -- what to go after manually and see if they

1 can break in using rainbow tables, you know,
2 "Password" is password, that kind of thing.

3 I don't really know specifically what
4 tools -- and -- and they don't really want us to
5 know that, right? Because that's part of their
6 secret sauce. How they get the information, we
7 don't really know. But once they get it, we get the
8 results.

9 Q. And do you recall what the results were
10 with respect to this testing?

11 A. Not specifically. I'm sure there was a
12 list much like the one we looked at before, where
13 they color code them and they kind of rank them as
14 far as criticality.

15 Q. And do you recall whether Fortalice
16 identified any vulnerabilities specifically with
17 respect to OLVR or MVP?

18 (Court reporter lost power.)

19 (Off the record.)

20 VIDEOGRAPHER: The time is 11:53. We're
21 back on the record.

22 BY MS. KAISER:

23 Q. So, Mr. Hamilton, we were discussing
24 Exhibit 6 [sic] before we went off the record.

25 Do you recall that?

1 A. Yes, ma'am.

2 Q. And including this email from Mr. Barrett
3 [sic] that talked about Fortalice getting "a good
4 understanding of any vulnerabilities of OLVR and
5 MVP."

6 Do you see that?

7 A. Right.

8 Q. And I believe we were discussing did
9 you -- do you know whether Fortalice identified any
10 vulnerabilities specifically with respect to OLVR
11 and MVP in 2020?

12 A. I -- I don't recall without being able to
13 look at the report. But I -- I think I stated
14 before, they're pretty good at what they do, so if
15 there was any to be found, they would have found
16 them. So...

17 Q. And if they found any, they would have
18 included that in their written report that was
19 delivered to the Secretary of State's office; is
20 that correct?

21 A. Correct.

22 Q. We can look at the next exhibit. I
23 believe it's Exhibit 6.

24 A. Okay.

25 Q. Yes, Exhibit 6.

(Plaintiffs' Exhibit 6 was marked for identification.)

BY MS. KAISER:

Q. Have you seen this document before?

A. Yep.

Q. And it looks like it's a task order from Fortalice to the Secretary of State's office; is that right?

A. Correct.

O. It's dated --

A. It's a -- what they -- what they refer to as a bucket of hours, yes.

Q. And this is dated -- dated March 11, 2021; is that right?

A. Correct.

Q. If you look on the second page, the signature line, is that your signature?

A. It is.

Q. So you approved this task order; is that right?

A. Correct. Statement of work, right.

Q. The project description is, "The following task order has been established to provide the Georgia Secretary of State with Chief Information Security Officer Support."

1 Do you see that?

2 A. Uh-huh.

3 Q. And then under -- at the bottom of that
4 table on page 1, the last line there says,
5 "Deliverables." It says, "Monthly report including
6 tasks accomplished by labor category."

7 Do you see that?

8 A. No --

9 Q. This is on page 1.

10 A. -- I don't, actually.

11 You're talking about -- oh, okay. Maybe
12 I'm looking -- under the table. I got it. Yep.

13 Q. Right.

14 To your knowledge, did Fortalice provide
15 monthly reports pursuant to this task order?

16 A. I would think they would have had to,
17 right, to be able to get paid. And those would have
18 went to Merritt. So...

19 Q. So you think those were provided to
20 Merritt Beaver?

21 MR. MILLER: Objection --

22 THE WITNESS: I'm sure.

23 MR. MILLER: -- foundation.

24 THE WITNESS: We should ask him, I guess.

25 Yeah.

1 BY MS. KAISER:

2 Q. Do you recall any situation during your
3 tenure at the Secretary of State's office in which
4 Fortalice was brought in to handle any potential or
5 actual breach of a security -- excuse me --
6 Secretary of State's system?

7 A. There were some incidents that they were
8 brought into, but nothing that -- nothing that rose
9 to the level of an actual breach.

10 Q. What do you recall about those incidents?

11 A. Just as a matter of course, you know,
12 we -- we'd find something or, you know, somebody
13 alerts us.

14 It's not uncommon for, you know, us to
15 bump into things on a daily basis that might be a
16 problem, so we usually vet them. And that's what --
17 this backs us up. It allows us to use them as a
18 subject matter expert to be able to hunt down stuff,
19 and they give us an opinion, a judgment, whether
20 it's real or not real or -- so...

21 Q. And does that trigger the incident
22 response plan that you described previously, if
23 they --

24 A. Yeah, only --

25 (Cross-talk.)

1 A. Only if it's deemed -- only if it's deemed
2 as a potential breach, right.

3 Q. And during your time, you don't recall any
4 incidents that were deemed a potential breach?

5 A. No, there was at least one, yep.

6 Q. What do you recall about that -- that one?

7 A. That was the one where John Q Public
8 emailed somebody in the agency that they found
9 something, which is not uncommon. I have that
10 happen in healthcare, too, where somebody from the
11 outside, you know, is -- is trying to tell you that,
12 "Hey, I found this problem. You want to fix it."

13 Most of the time, it's -- it has been my
14 experience that it's a -- it's a regular good guy
15 that's doing the right thing, just trying to be part
16 of the Internet community.

17 But I think here at State they were a
18 little paranoid of that, with all the media pressure
19 and things like that. My opinion again.

20 So we elevated it to them to do a little
21 background on it to make sure that we were flying in
22 the right direction. So...

23 And there were -- there were some things
24 that were found that didn't directly line up with
25 what they said that we got our vendor to address in

1 a big hurry.

2 But, you know, I -- I never turn away
3 anyone from the public telling me something,
4 because, you know, we're all in this together. So
5 if somebody sends an email to somebody in the
6 agency, I vet it, because it could be right. You
7 never know. So...

8 Q. Do you recall approximately when this
9 incident took place where you received an email from
10 somebody in the public?

11 A. Probably 20- -- probably in 2021, early
12 2021 or late '20.

13 Q. And did the potential vulnerabilities that
14 this person, the member of the public, emailed you
15 about pertain to the election system?

16 A. The registration site, right.

17 Q. And so in response, you asked Fortalice to
18 take a look; is that right?

19 A. Correct.

20 Q. And they did identify some -- some real
21 issues?

22 A. They did.

23 Q. What steps were taken to remediate those
24 issues?

25 A. A code line change by the vendor to -- to

Page 89

1 flush a certain variable to make it null set instead
2 of just a sequential number.

3 Q. Who was the vendor at that time?

4 A. PCC or whatever they called themselves
5 after the fact.

6 Q. Were there any steps taken to ensure that
7 the vulnerability had been -- had not been utilized
8 by a bad actor, for example?

9 A. Yeah, there was some -- there was some
10 logging available on the site, but it was
11 ascertained by Fortalice that it wasn't a bulk
12 situation. It was a situation where you would go to
13 the website and you'd look at the -- at the data in
14 the URL line and you'd notice that it was, you know,
15 serialized, 1234. And if you put 1233, it would
16 then display the last guy that was in.

17 So it didn't go any further back than that
18 and it didn't go forward, so for somebody to -- to
19 use that tool, it would have taken forever to get,
20 you know, any substance.

21 But it was definitely an issue, so we took
22 care of it. I say "we." We asked that it be taken
23 care of.

24 MS. KAISER: Tab 16.
25

1 BY MS. KAISER:

2 Q. You should see an exhibit, Exhibit 8.

3 (Plaintiffs' Exhibit 8 was marked for
4 identification.)

5 THE WITNESS: Okay.

6 BY MS. KAISER:

7 Q. If you -- if you start from the last email
8 in the chain, it looks like it's from August 12,
9 2020, from Kijyuu Tradebit.

10 Do you see that?

11 A. Yeah, I do. I got it.

12 Q. Does this document describe the incident
13 you were just talking about?

14 A. Yeah, it would be a good example of -- of
15 one that we got from the outside, right.

16 Q. Okay.

17 A. Yep, that's the one. The --

18 Q. This is the one --

19 A. -- randomization of the last four digits,
20 right.

21 Q. Right.

22 So this came from somebody in the public
23 who wanted to stay anonymous; is that right?

24 A. Right.

25 Q. They contacted the Secretary of State's

1 office because they identified this vulnerability
2 with the voter registration system.

3 Do you see that?

4 A. Right.

5 Q. And this was with the Cobb County voter
6 registration system.

7 A. Uh-huh.

8 Q. Do you recall that?

9 A. Yep.

10 Q. So this email went to Michael Barnes, who
11 then forwarded it to you; is that right?

12 A. Correct.

13 Q. And did you interact with this individual
14 who reported the vulnerability?

15 A. I'm not sure if I actually emailed. I
16 might have emailed this person. I'm not sure.

17 But just on the face of it, I think I
18 kicked off, you know, a process internal to kind of
19 review it and go look and see what they were looking
20 at.

21 It -- it's certainly not uncommon to have
22 folks from the public say, "Hey, we got this wrong."
23 You know, as I said, it's -- even in healthcare
24 today, we still have those. And some of the ones we
25 follow -- you know, we follow up on, there's a real

1 problem; others, not so much.

2 So I don't want to waste anybody's time,
3 but usually they don't go into such a big deal of,
4 you know, obfuscation of who they are. That was a
5 little weird.

6 So we definitely looked into this one, and
7 it ended up that this one had a problem, but it was
8 actually on the Cobb County side of things. And so
9 I -- I reached out for -- for the IT folks on their
10 side and -- and, you know, alerted them to it,
11 and -- and the IT director over there took the site
12 down, took it off the air, until they could get the
13 code line remediated.

14 And it -- it was basically pointing only
15 to their Cobb County information, so, you know, it
16 was up to them. We're just trying to be good
17 citizens that "we heard something and here we go."
18 It wasn't uncommon for us to have discussions with
19 the counties, because they all operate independently
20 from the Secretary of State. So...

21 Q. Right. And you can see that in your
22 email -- this is on page 2 of the document; the
23 Bates number is -126679 --

24 A. Yeah. Okay.

25 Q. -- you emailed -- in the middle of the

1 page there, you emailed Kimberly Lemley.

2 Do you see that?

3 A. Yeah. I don't know her personally, but,
4 yeah, that was the IT person. Director, I think it
5 was, yeah.

6 Q. All right. And you -- you reported that
7 this appeared to be a valid vulnerability.

8 You see that?

9 A. Correct.

10 Q. Okay. And so -- and to your knowledge,
11 Cobb County addressed this particular vulnerability;
12 is that right?

13 A. Yeah. They pulled the site down pretty
14 quickly after I sent this email and -- yeah.

15 Q. If you go back to page 3 of the document,
16 there's an email from you in the middle of that page
17 from Wednesday, August 12 --

18 A. Right.

19 Q. -- to Merritt Beaver and others. It says,
20 "Here it is. He is right, I checked. It sounds
21 like the same thing -- the exact same thing we
22 addressed with PCC on our website."

23 Do you see that?

24 A. Right.

25 Q. What did you mean by that?

1 A. Yeah, it's a -- just a common web
2 vulnerability, is that they do insertion at the
3 actual URL line. Same issue that comes up on a lot
4 of things, so not uncommon.

5 Q. And when you say "our website" --

6 A. It would have probably -- I was most
7 likely referring to either MVP or the OLVR.

8 I think the difference was -- is that
9 we -- I think we caught that one internally. So...

10 Q. Did you take steps to remediate that one?

11 A. Yeah, again, just reach out to the
12 developer and have them change the way they
13 randomize that number.

14 Q. I'm going to add Exhibit 9.

15 A. Okay.

16 (Plaintiffs' Exhibit 9 was marked for
17 identification.)

18 THE WITNESS: Okay.

19 BY MS. KAISER:

20 Q. So this looks to be an email chain from
21 the same time period, August 12, 2020.

22 A. Right.

23 Q. It starts with the same email from Kijyuu
24 Tradebit. But I just want to focus on your email at
25 the top of page 1.

Page 95

1 A. Right.

2 Q. This is an email from you to Nick Salsman,
3 Ronnell Spearman, and Derek Hawkins.

4 Do you see that?

5 A. Correct. Those are the three security
6 people on my team.

7 Q. And you say, "Guys, I would like to see if
8 the other big counties have similar sites that have
9 this vulnerability."

10 Do you see that?

11 A. Yes.

12 Q. You ask them, "Would you nose around
13 Fulton, Gwinnett, DeKalb, Forsyth, et cetera and see
14 if this developer possibly sold the same app to
15 them?"

16 Do you see that?

17 A. Correct.

18 Q. Do you know if your -- these team members
19 did that review?

20 A. They did.

21 Q. What did they find?

22 A. None of the counties they tested had the
23 same vulnerability.

24 Q. Did you only test these about five
25 counties?

1 A. Right. Because we have 159 counties in
2 Georgia. Right. It would be a manual test.

3 Q. So you didn't --

4 A. You'd have to go find out every single
5 test and -- but usually it's only the big counties
6 that have the money to do their own site instead of
7 just forwarding it to the MVP or the OLVR.

8 So I just told them to hit the big ones
9 just to make sure. And that was just a -- truly a
10 community thing. We just wanted to make sure that
11 everybody was safe, not just us.

12 Q. Were there -- was anything else done to
13 ensure that other counties didn't have this same
14 vulnerability?

15 A. No, I think that was it. We just -- I had
16 the guys do some vetting of those sites, and if --
17 if one of them had come up, we would have done the
18 same thing that we did with Cobb. We would have
19 reached out and said, "You need to down your site
20 until you get this fixed."

21 Q. Previously, Mr. Hamilton, you gave some
22 answers about the fact that, you know, security is a
23 journey --

24 A. Yeah.

25 Q. -- not a destination and it involves, you

Page 97

1 know, prioritizing certain remedies and that kind of
2 thing. I just wanted to go back to that for one
3 minute.

4 A. Sure.

5 Q. You would agree that the --

6 A. Sure.

7 Q. -- Secretary of State is responsible for
8 what's considered critical infrastructure, including
9 the election system, would you not?

10 A. Yes.

11 MR. MILLER: Objection. Lack of
12 foundation. Calls for speculation.

13 BY MS. KAISER:

14 Q. And do you agree that all reasonable
15 measures should be made to secure such critical
16 systems?

17 MR. MILLER: Same objection.

18 THE WITNESS: Reasonable, right, yep,
19 reasonable and appropriate. It's all based on
20 judgment.

21 BY MS. KAISER:

22 Q. So you were not suggesting that it's
23 appropriate to leave significant vulnerabilities
24 unmitigated when you're dealing with --

25 (Cross-talk.)

1 A. Not at all.

2 Q. -- critical infrastructure?

3 MR. MILLER: Objection.

4 THE WITNESS: Not at all.

5 BY MS. KAISER:

6 Q. And you were not suggesting it's
7 appropriate to take no measures to mitigate
8 significant vulnerabilities with critical
9 infrastructure systems?

10 MR. MILLER: Same objection.

11 THE WITNESS: Correct, I was not. If we
12 can't fix it one way, there's usually other
13 compensating controls that we can do. So...

14 BY MS. KAISER:

15 Q. I have a couple of questions about
16 Georgia's prior election system, by which I mean the
17 DRE voting system.

18 A. Oh, yeah. I probably won't be much --

19 Q. Are you aware of any --

20 A. -- help there, but --

21 Q. Are you aware of any efforts made by
22 anyone in the Secretary of State's office to
23 determine whether malware was located on any
24 component of the -- of the prior DRE system?

25 MR. MILLER: I'm going to note an

1 objection on relevance here.

2 And, Mary, if you'll just allow me the --
3 humor me to have a running objection on this
4 line of questions for the old system.

5 THE WITNESS: Yeah, I wasn't around then,
6 so I just don't have any personal knowledge.

7 BY MS. KAISER:

8 Q. What components of the DRE system were
9 carried over or used at any point in time with the
10 new voting system, the BMD system?

11 MR. MILLER: The same objection. Lack of
12 foundation.

13 THE WITNESS: I -- I don't really know
14 what was there before; I can only tell you what
15 was there when I got there. So...

16 BY MS. KAISER:

17 Q. So you don't have any knowledge about
18 whether equipment or servers were reused?

19 A. I think initially they probably reused the
20 servers while they were waiting to put in the new
21 ones. But that's just a piece of hardware. So...

22 At -- at one point, PCC, the company, had
23 the responsibility for the operations side, and when
24 that transferred to the Secretary of State, there
25 was a big refresh of hardware that came with it.

Page 100

1 Q. Do you recall about when that took place?

2 A. Pretty soon to the beginning of my
3 engagement. It was probably sometime 2018, early
4 2019. That's a guess, but yeah.

5 Q. You said they probably initially reused
6 servers while waiting to put in new ones.

7 Do you know when the new servers were put
8 in -- put into place?

9 A. I -- I don't have a date. That would be a
10 question for Merritt. He probably would remember
11 the date.

12 Q. Are you aware of any situation where there
13 was a suspected hack of any aspect of the IT system
14 that the Secretary of State has responsibility for?

15 A. No, not -- I -- I mean, it's a terminology
16 thing.

17 I know -- I think what you're talking
18 about is a bad actor hacking. There are good
19 actors, like Fortalice, that does good hacking.
20 But, no, not from a bad side, no.

21 Q. Other than Fortalice, are you aware of
22 any -- any hacks, good or bad?

23 A. No. We -- we monthly used our own tool,
24 Qualys, to interrogate a lot of the websites
25 internally. But that was for our own use, just to

1 make sure things were prodding along.

2 For instance, like the statement that I
3 made before about something being remediated, that
4 was a snapshot in time. So if something changed the
5 next day, a new release, something happened in the
6 real world, then you -- that's -- that's why you --
7 you kind of keep a -- a good -- a good bead on
8 everything that's happened in the past and you keep
9 retesting it all the time just in case. So...

10 Q. Are you aware of any incident where there
11 was unauthorized access to any aspect of the IT
12 infrastructure that the Secretary of State's office
13 manages?

14 A. No, not -- not directly.

15 Q. Are you aware of any attacks on election
16 infrastructure in any counties in Georgia?

17 MR. MILLER: Objection. Lack of
18 foundation.

19 THE WITNESS: Yeah, I -- I wouldn't know
20 about the counties because they didn't kind of
21 report up through me. It's two separate
22 entities.

23 But as far as the -- the home-based
24 system, what we were responsible for, no.

25 BY MS. KAISER:

Page 102

1 Q. Exhibit 10.

2 A. Yeah, I got it.

3 (Plaintiffs' Exhibit 10 was marked for
4 identification.)

5 BY MS. KAISER:

6 Q. I'll represent to you that this is a news
7 article.

8 Do you -- do you recall this -- I'm sorry.

9 The news article describes a ransomware
10 attack on Hall County election infrastructure in
11 October 2020.

12 Do you see that?

13 A. Yep.

14 Q. Do you have any recollection of that
15 incident?

16 A. Vaguely. I remember folks talking about
17 it, but we didn't get involved in it.

18 Q. And by "we," you mean the Secretary of
19 State's office?

20 A. Correct. Right.

21 Q. So if the Secretary of State's office was
22 not involved in any investigation or -- or
23 remediation in --

24 A. No. My recollection of this event is it
25 just hardened our -- our intent to kind of get out

Page 103

1 in front of people within our organization to
2 reeducate them on a monthly basis about the dangers
3 of ransomware and don't click the link if you don't
4 absolutely have to and things like that.

5 I spent a lot of my time kind of
6 evangelizing security and even made some videos for
7 the organization that could be played at any time,
8 not just on shift.

9 So we had pretty good tools at the
10 Secretary of State that allowed us to, you know,
11 keep away from that kind of stuff. The -- the
12 smaller counties may not have the budget to do that.
13 That would be my opinion. So...

14 Q. Are you aware of any incident where
15 somebody contacted the Secretary of State's office
16 and threatened to hack Georgia's elections?

17 A. No. I mean, I -- I don't -- nothing
18 directly that I -- that I saw or -- no.

19 Q. If something like that happened, would
20 it -- would it fall under your responsibility to
21 respond to that?

22 A. I would imagine that somebody in
23 leadership would have tipped me off to it as to, you
24 know, "Here, go look at this. Somebody thinks we're
25 a ripe target" kind of thing. But I don't remember

Page 104

1 any specific instances where Merritt or somebody
2 came to me and said, "Hey, somebody's going to hack
3 us."

4 So I -- honestly, as a security
5 professional, I think the world's going to hack me
6 every day. That's how I go to work. So... They
7 only have to be right once. I've got to be right
8 every day.

9 Q. Understood.

10 MS. KAISER: Can you publish Tab 8,
11 please.

12 (Plaintiffs' Exhibit 11 was marked for
13 identification.)

14 BY MS. KAISER:

15 Q. We're adding I think what will be
16 Exhibit 11.

17 All right. Do you have Exhibit 11 open,
18 Mr. Hamilton?

19 A. I do.

20 Q. The first email in this chain is from
21 Bret Hadley.

22 Do you see that?

23 A. Gotcha. Yep.

24 Q. April 4, 2019?

25 So this is --

1 A. Got it.

2 Q. -- during the time that you worked with
3 the Secretary of State's office; is that right?

4 A. If it was sent in April -- oh, yeah, okay.
5 I would have -- I don't know if I was on site that
6 week.

7 Because that was -- if they copied Clark
8 Rainer, he was the IT director at that point, and it
9 was when he left that I started spending a little
10 more time at Secretary of State. So this might have
11 been maybe one of my off weeks where I was at
12 another client.

13 Q. Okay.

14 A. I don't remember this email, seeing it, I
15 don't think. I don't...

16 Q. Okay. Yeah.

17 So Mr. Hadley's email at the bottom of the
18 page, the subject is "I bet I can hack your election
19 [sic] voting machines."

20 Do you see that?

21 A. Yeah.

22 Q. He said, "If you don't want me to try and
23 hack your elections, please follow Oregon's lead and
24 vote by mail, on paper. You really DON'T" -- all
25 capitalized -- "need electronic voting machines, but

1 if you insist, then let the games begin. Fair
2 warning."

3 Do you see that?

4 A. Yep.

5 Q. And it looks like -- it looks like this
6 was sent to soscontact@sos.ga.gov?

7 A. Right. That's just the -- the basic
8 website. It's like sending a note to the webmaster,
9 right.

10 Q. Okay. And then this was forwarded on to a
11 group of people, including -- let's see -- including
12 Chris Harvey and Kevin Rayburn.

13 Do you see that?

14 A. Yep. James Oliver. Right.

15 Q. Right.

16 But you don't recall -- you don't have any
17 recollection of this email or this incident?

18 A. No, ma'am.

19 Q. And you don't recall any similar threats
20 during your time at the Secretary of State's office?

21 A. No, nothing like that. It's been my
22 experience that people who threaten usually don't do
23 it. It's the people that don't say anything that do
24 things like this.

25 Q. Do you know whether there has ever been a

1 cybersecurity assessment done of Georgia's voting
2 equipment?

3 A. I do not. As I understood it, that was
4 the privy of the Dominion folks and that they were
5 independently certified. I don't know much about
6 that process.

7 Q. So you're not aware of any cyber
8 assess- -- cybersecurity assessment of the voting
9 machines?

10 A. No, ma'am.

11 Q. Are you aware of any reports or
12 conclusions regarding any security vulnerabilities
13 with the BMD system?

14 A. Not -- not specifically, because it kind
15 of fell outside my scope. So...

16 Q. Are you generally aware of any?

17 A. No, I -- I can't recall any that -- I
18 mean, there was always the underpinnings of somebody
19 trying to do something, but we live with that every
20 day. So...

21 Q. So you're not personally aware of any
22 security breaches or vulnerabilities involving the
23 BMD system.

24 MR. MILLER: Objection. Asked and
25 answered. Lack of foundation.

1 THE WITNESS: Yeah, I -- not that I can
2 recall.

3 BY MS. KAISER:

4 Q. Are you aware of any complaints regarding
5 the security of the BMD system?

6 A. No. I -- I think I read some news stories
7 and things like that, but nothing specific.

8 Q. What is the Election Center?

9 A. I think that's the hardened facility that
10 they moved to. I've never been in it. Not meaning
11 like moved the servers to. I think that was like
12 the -- the war room, so to speak. It's where the
13 people went during an election.

14 Q. The people but not the servers, you said?

15 A. No. Servers are maintained in -- in
16 secure data centers.

17 Q. Okay. What server is the election
18 management system for the new BMD election system,
19 where is that currently hosted?

20 MR. MILLER: Objection. Foundation.

21 THE WITNESS: Yeah, I can only -- I can
22 only speak to the stuff for the election side
23 of the house for the registration side, and
24 those are housed in -- here in Atlanta, and
25 then there's -- there's a backup site that gets

Page 109

1 mirrored in Ashburn, Virginia. Both of them
2 are QTS sites, Quality Technical Services.

3 BY MS. KAISER:

4 Q. Is there a point in time that there --
5 that the election management system for the new --
6 for the BMD voting system was moved to a new server?

7 MR. MILLER: Objection. Lack of
8 foundation.

9 THE WITNESS: Again, for the BMD site, I'm
10 not -- I'm not sure. I can only --

11 BY MS. KAISER:

12 Q. You weren't involved in that?

13 A. -- speak to ENET -- ENET and, you know,
14 MVP sites, things like that.

15 (Off-the-record discussion.)

16 THE WITNESS: 12 is the new one?

17 BY MS. KAISER:

18 Q. Do you have that up?

19 (Plaintiffs' Exhibit 12 was marked for
20 identification.)

21 THE WITNESS: Oh, EMS? Yeah.

22 BY MS. KAISER:

23 Q. Yeah. So this is an email chain from
24 July 15, 2020.

25 Do you see that?

Page 110

1 A. Right.

2 Q. The first email is --

3 A. Right. This is --

4 Q. -- from you?

5 A. Right. This is the system that does the
6 ballot design.

7 Q. Ballot design. Okay. Yeah.

8 So the subject is "EC Visit Notes."

9 What does "EC" stand for?

10 A. Election Center in Marietta.

11 Q. Okay. And you say this is what does the
12 ballot design.

13 What program does the ballot design?

14 A. I'm not sure who authored it. It was
15 something that was -- that was originally installed
16 on a -- on a private network, not facing the
17 Internet, and great -- great care was taken to make
18 it not touch the Internet. So we basically
19 constructed a -- a new virtual environment for it,
20 and it, as far as I know, remains that way today.

21 But I don't remember that as BMD. I
22 remember it as the -- that EMS system.

23 Q. Right. And "EMS" being the Election
24 Management System; is that right?

25 A. Yeah, I think that's what they call their

Page 111

1 ballot design thing. I think that's -- that's
2 all -- what we likingly call Michael Barnes'
3 servers, right. That was it.

4 Q. All right. So the EMS system is used for
5 the ballot design, and that's true with respect to
6 the new BMD voting machines, too; right?

7 A. Yes. It's just, I think, a different
8 version. Because it didn't run on the -- on the
9 version of Virtual Center that we had, so we had to
10 upgrade that environment. And that was what this
11 project was about, just trying to get out of their
12 way so they could get the new thing set up.

13 Q. In the second line of this email, you say,
14 "I do think the shortest path is to spin up an
15 additional VM host on 6.5, build everything
16 new - partition the existing storage, add some
17 drives."

18 Do you see that?

19 A. Right.

20 Q. Can you -- can you explain what you meant
21 there?

22 A. VM host is -- is -- a host is a -- is a --
23 is a set of software that runs on a physical server
24 that allows you to spin up independent guests, which
25 are instances of servers that run in a virtual

1 world.

2 So being that they were way back at
3 Version 5.2, we needed to get them on the most
4 current version to be supported even though it was
5 off the Internet, just because it was the -- you
6 know, the right thing to do, get on the latest code
7 line for -- with the virtualization side of things
8 so they could run their servers.

9 Q. Who do you mean by "they"?

10 A. Michael Barnes' group. He's got a group
11 of people out there, half a dozen folks.

12 Q. And your next line says, "This" -- sorry.
13 The next line down says, "This would give us a clean
14 slate."

15 A. Right.

16 Q. So you thought this was the right way to
17 go because it would basically allow you to start
18 over --

19 A. Right, the --

20 Q. -- with the EMS system; is that right?

21 A. -- the idea being that the servers had
22 some age on them and the -- you know, the operating
23 systems that they ran had some age, so we wanted to
24 get them on something current.

25 Because I think there was some assumptions

Page 113

1 made that if it had new software, we're going to
2 have to have the underpinnings be that way as well.
3 So, yeah, this was one of many recommendations I
4 made for that environment.

5 Q. Was that recommendation followed?

6 A. Yes. It was actually my team that ended
7 up building it, because the infrastructure team was
8 otherwise engaged in spinning up other things. So
9 my team took it on -- upon themselves to get that
10 set up.

11 Q. The last line of your email says, "Lots of
12 open stuff to make us security folks nervous - but
13 out of all we do - this likely needs to be the most
14 secure."

15 Do you see that?

16 A. Correct. Correct.

17 Q. Why did you feel that this needed to be
18 the most secure?

19 A. Because historically, it had been an
20 off-net, private net solution, so you knew they were
21 nervous about it being on the edge.

22 All the other things that we were
23 responsible for were public-facing, a lot of public
24 information. This was not public information. This
25 was to help the 159 counties do ballot design and

1 things like that.

2 So, yeah, out of all the things we did,
3 this was probably the most critical.

4 Q. If you look at Kevin Robertson's response
5 to you, the top of page 1.

6 A. Okay.

7 Q. And who is Kevin Robertson?

8 A. He was the head of the I- -- what we would
9 term as a PMO, project management office. So...

10 Q. Did you work with him on this project?

11 A. Yes, yes. He -- we worked together on a
12 lot of different things. He kind of was the
13 right-hand guy of Merritt.

14 Q. Okay. Number 3 in Mr. Robertson's email
15 here says, "Once we copy everything over then
16 determine if we want to use the existing servers and
17 build those out with new patches and recommendations
18 made in the attached survey."

19 Do you see that?

20 A. Right.

21 Q. Was Mr. Robertson suggesting using
22 existing servers rather than new ones?

23 A. He was, but he didn't understand that the
24 newest code wouldn't run on the older servers. So
25 oil and water.

1 Q. And so, ultimately, you did use new
2 servers?

3 A. Correct.

4 Q. And let's see. These emails were from
5 June 2020.

6 Do you know when that change was made,
7 when the new servers went into use?

8 A. I think probably by the end of the year,
9 there was -- he had a due date. I don't know if he
10 mentioned it on here. Michael is -- no, not on this
11 one.

12 Michael usually waited till the last
13 moment to let us know. So I -- I'm not sure how
14 fast we were able to turn that thing around for him,
15 but I do think we hit his date. Otherwise, the
16 world would have stopped turning, according to
17 Michael. So...

18 Q. Understood.

19 If you look at item 2 in Mr. Robertson's
20 email --

21 A. Uh-huh.

22 Q. -- it says, "Reached out to Dominion and
23 set the expectation that they are going to load what
24 is needed once we build out the environment."

25 Do you see that?

Page 116

1 A. Correct.

2 Q. Do you know what he meant by that?

3 A. The actual specific software that goes on
4 there we did not have any experience with, so I
5 think I had asked somebody along the line, I said,
6 "If -- if the vendor should do the install, then let
7 them do the install."

8 But I would do that with other examples,
9 too. That's probably where that came from.

10 Q. And when you mean [sic] "the software,"
11 you mean the actual EMS software that did --

12 A. Correct.

13 Q. -- the ballot design?

14 A. Yeah. Yeah. So in other words, right,
15 you've got a Windows -- a Windows box that runs
16 Windows and on top of that are individual
17 applications. This would be an individual
18 application on top of that.

19 (Plaintiffs' Exhibit 13 was marked for
20 identification.)

21 BY MS. KAISER:

22 Q. Can you look at the next exhibit, 13?

23 A. Okay. Hang on. Oh, I don't have that one
24 yet. Hang on.

25 All right.

1 Q. And I'll represent to you this was an
2 attachment to the prior email that we were just
3 looking at.

4 A. Right.

5 Q. This -- so it says "Site Visit."
6 "Election Office Notes" --

7 A. Right.

8 Q. -- "10am 6/15/20 Meeting."

9 You see that?

10 A. Right.

11 Q. And did you recall this meeting -- I
12 mean -- sorry -- do you recall attending that
13 meeting?

14 A. Vaguely, yeah. I -- I definitely -- this
15 would be like one of my normal hit lists that I list
16 when I go somewhere. Yep.

17 Q. So do you think that these are notes that
18 you took at that meeting?

19 A. Yes.

20 Q. What was the purpose of the meeting?

21 A. To get a feeling for where he is today and
22 where he wanted to be and how much of a heavy lift
23 it was going to do to -- to get it running.

24 Q. And when you say "he," you mean --

25 A. Michael Barnes. I'm sorry. Yeah.

1 Q. So this was kind of the level set about
2 the project of getting the new servers going for the
3 EMS --

4 A. Right.

5 Q. -- software?

6 A. This was the feedback to the PMO so they
7 could break it into tasks and figure out what other
8 groups needed to help.

9 And some of the errata I put in here was
10 just typical security guy, head on a swivel, you
11 know, walking around the facility, things I noticed
12 that we could do better. So just a heads up.

13 And, you know, the idea of giving it back
14 to the PMO would be so he could kind of filter it
15 through the different groups of responsibility.
16 So...

17 Q. Under "Basic Overview," about -- I think
18 it's about eight bullets down, it says, "No patching
19 of VMware in recent memory, no firmware updating of
20 the hosts, controllers, network gear, etc."

21 Do you see that?

22 A. Correct. Yeah.

23 Q. What did you mean by that?

24 A. Because it was off-net, they had no way to
25 patch it. They didn't know how, let's put it that

1 way.

2 Q. And was that a concern to you?

3 A. Yeah. I mean, I -- I just -- I looked at
4 it as any other asset. I mean, that's what we do is
5 we make judgments based on the asset and also the
6 criticality of the data that's on it.

7 Not so much from a security standpoint,
8 but if you're not on the most current versions of
9 software, firmware, things like that, if you end up
10 having a problem and you end up calling anybody for
11 support, they're going to -- the first question out
12 of their mouth is going to be, "Are you on the
13 current version?" And if you're not, then they're
14 going to say, "Call us back when you are." So that
15 was my -- one of my concerns.

16 It -- back to that confidentiality,
17 integrity, and availability. That's that
18 availability and integrity side of the house that I
19 was trying to lay into.

20 Q. Can you flip to the next page?

21 A. Okay.

22 Q. At the top under "Application Related,"
23 the first bullet point --

24 A. Right.

25 Q. -- it says, "Legacy 1998 Application -

Page 120

1 GEMS - now defunct. Now supported by Dominion."

2 Do you see that?

3 A. Right.

4 Q. What did you mean by that?

5 A. I guess "GEMS" refers to a company name.

6 I don't know if it was a company name or a product.

7 And this was basically notes from a meeting, so this
8 is probably what Michael Barnes told me.

9 Q. Do you know what "GEMS" is?

10 A. I'm sure the acronym spans a lot of
11 things, but I don't recall pursuant to this.

12 Q. Do you recall if it -- do you have any
13 recollection that it is the -- the prior Election
14 Management System that was used with the DRE system?

15 MR. MILLER: Objection.

16 THE WITNESS: I didn't --

17 MR. MILLER: Asked --

18 THE WITNESS: -- no.

19 MR. MILLER: -- and answered. Lack of
20 foundation.

21 COURT REPORTER: Could you repeat your
22 answer, please?

23 THE WITNESS: I don't. I'm sorry.

24 COURT REPORTER: Just remember to speak
25 one at a time so --

Page 121

1 BY MS. KAISER:

2 Q. So you don't --

3 MS. KAISER: Sorry, Ms. Barnes. Thank
4 you.

5 BY MS. KAISER:

6 Q. So you don't know what it meant that
7 the -- that GEMS was now supported by Dominion?

8 MR. MILLER: Objection. Lack of
9 foundation.

10 THE WITNESS: I didn't take that away, I
11 guess, from that meeting. I was just -- I was
12 focused on getting the new stuff loaded.

13 BY MS. KAISER:

14 Q. A few bullets down says, "No history of
15 patching anything," and that looks like a frowny
16 face next to it.

17 A. Yeah. I can do one --

18 Q. What did you mean --

19 A. -- right here.

20 Q. What did you mean by that?

21 A. It's just a -- it's -- it's basically
22 repeating what he told me. He says there's no --
23 there's no history of patching anything.

24 Because there was an assumption that it
25 was off-net, it didn't need to be patched. The

Page 122

1 reason people patch is because they're afraid of the
2 Internet. It's not on the Internet; we don't need a
3 patch.

4 That's not necessarily the way I think,
5 so -- you still gotta be current for the support
6 reasons.

7 Q. So why did you include a frowny face after
8 that comment?

9 A. Just -- it's kind of -- for me, when I see
10 a frowny face, it's to kind of remind me that that
11 was a bad thing. Just a note-taking style.

12 Q. So that was something that you thought
13 needed to be changed?

14 A. Yes.

15 Q. Two bullets down from that, it says, "Need
16 to be able to scan every USB attached storage device
17 connected to prior [sic] use. Cannot ensure USB is
18 free from malware, keylogging, etc."

19 Do you see that?

20 A. Yes.

21 Q. What did you mean by that comment?

22 A. So it was common practice for the -- for
23 the data to be shared with the counties once they
24 drafted or came up with a -- a strawman of what
25 their ballot looks like. They would share that data

Page 123

1 via USB. They would, you know, FedEx it to them and
2 then they'd -- they'd mark up changes and then
3 they'd FedEx the USB key back.

4 Even though Michael had an internal
5 process that when he started the event, he would
6 take a USB drive out of the package and start, he --
7 he thought that was good enough and -- because he
8 encrypted it and did a lot of other things.

9 But, you know, I had a different
10 experience in life, so I decided that I thought that
11 he needed to go to a more secure managed solution
12 for USB drives, and I proposed moving to a -- an
13 actual managed USB key program.

14 And I'm not sure if that ever got funded
15 or not. It was not an insignificant amount of
16 money, but I think they decided that the -- you
17 know, the juice wasn't worth the squeeze, so to
18 speak.

19 Q. So to -- to your knowledge, at the time
20 you left the Secretary of State's office, that
21 recommendation had not been implemented --

22 A. No. They had -- they had quotes -- we had
23 quotes and we actually had sample units that Michael
24 Barnes had where he was using it for his work flow
25 to see how it moved.

Page 124

1 But I think I left before that decision
2 was made. So...

3 Q. And why did you make that recommendation?

4 A. Because he was using commodity-based USB
5 drives.

6 Q. And why was that not a best practice, in
7 your view?

8 A. Because they're not made in the U.S.

9 They're -- they could have all kinds of things on
10 them. We don't know.

11 The only way to really make sure is to,
12 you know, wipe the thing free of -- it has to go
13 through a process of sanitization before you use it.

14 And, you know, I just -- I really like the
15 idea of a managed USB. The name of it is called
16 DataLocker, and -- and it actually has code on it
17 that you're able to track, much like a LoJack, and
18 it keeps a log of every file ever written and a
19 log -- a file of every -- every time it's read,
20 every time it's loaded, every time anything happens
21 to it, and it uploads it to a cloud-based service so
22 you can see where these drives are; and if someone
23 got ahold of one of these drives and put it in a USB
24 slot that wasn't authorized, that it would wipe the
25 contents securely and -- kind of like brickling a Mac

Page 125

1 if you don't -- if you're not the owner kind of
2 deal.

3 But it was a pretty significant outlay of
4 cash to get that done. And I think he liked the
5 idea. I think -- he wasn't as paranoid as I was.
6 Michael Barnes. Sorry. Didn't mean to say "he."

7 MS. KAISER: Can you add Exhibit 12,
8 please -- Tab 12?

9 THE WITNESS: 14.

10 (Plaintiffs' Exhibit 14 was marked for
11 identification.)

12 BY MS. KAISER:

13 Q. If you look at the first email in this
14 chain, it's from Michael Smith at DataLocker.

15 Do you see that?

16 A. Yeah, all the way at the bottom? Got it.
17 Okay.

18 Q. Is this the vendor that you were just
19 discussing?

20 A. Yes, ma'am.

21 Q. So it looks like in July of 2020, you
22 reached out to DataLocker and they sent you a
23 response.

24 A. Correct.

25 Q. And then your email at the top of

Page 126

1 page 1 --

2 A. Yep.

3 Q. -- you responded to Michael Smith?

4 A. Right. Talked about two use cases.

5 Right.

6 Q. And so this was your explanation of why
7 you were interested in using DataLocker?

8 A. Correct.

9 Q. And under -- under item 1 there, you say,
10 "We have a group in the Election Center that uses
11 consumer grade USB flash drives and software
12 encryption to move data regarding ballots and poll
13 information (not votes) to and from the 159 counties
14 in Georgia."

15 Do you see that?

16 A. Correct. I do.

17 Q. Further -- in the next -- top of the next
18 paragraph, you say, "Today these drives are erased
19 and loaded at the EC...."

20 Do you see that?

21 A. Right.

22 Q. Is that the Election Center?

23 A. It is. Marietta, right.

24 Q. It says, No. 2, "The environment where
25 these drives are initially populated is currently

Page 127

1 air gapped, and my group is reengineering the way
2 that it interacts with the world - maintaining its
3 logical and physical separation."

4 Do you see that?

5 A. Correct. Right.

6 Q. And so the environment that you're talking
7 about there, that's the EMS system that was on
8 the --

9 A. (Nodded head.)

10 Q. Yeah. Okay.

11 A. Correct. Yeah.

12 Q. -- that was in the Election Center.

13 So were people in the 159 counties using
14 USB drives to move data in and out of the air-gapped
15 EMS system?

16 MR. MILLER: Objection. Lack of
17 foundation.

18 THE WITNESS: Well, yes, but they were
19 provided by Michael's -- Michael Barnes' group.
20 I mean, it's not like the counties are going
21 out and buying their own and using them. It
22 was stuff that was originally provided by
23 Michael. So...

24 BY MS. KAISER:

25 Q. But they were using USB drives,

1 removable --

2 A. Correct.

3 Q. -- media.

4 A. Uh-huh.

5 Q. Is that consistent --

6 A. Yeah.

7 Q. -- with best practices, in your view?

8 MR. MILLER: Objection. Lack of
9 foundation. Calls for opinion testimony.

10 THE WITNESS: Yeah, it's -- it -- it's one
11 step above a sneakernet. So, yeah, I mean, I
12 understand why they did it. They didn't want
13 to use email -- I get it -- and they figured
14 that the courier system was more secure and the
15 encryption of the drives and -- you know, he
16 had an erasure kind of process that he went
17 through that we helped kind of tune up a little
18 bit so it does more of a wipe -- a DoD wipe of
19 a drive prior to use.

20 So it's just -- it's how he had done it
21 for years, and trying to change that was a bit
22 of a challenge.

23 BY MS. KAISER:

24 Q. Based on your experience and training, you
25 recommended that the Secretary of State use a vendor

Page 129

1 like DataLocker and implement a more secure process;
2 is that right?

3 A. Correct, yeah. Yeah, if you're going to
4 use a USB drive, it might as well be a managed,
5 FIPS-compliant device, right.

6 Q. If we can go back for a moment to
7 Exhibit 13.

8 A. Okay.

9 Q. I'm just finishing off looking through
10 your notes here.

11 This is on page 2 --

12 A. Okay.

13 Q. -- under "Operational" --

14 A. Okay.

15 Q. -- the second bullet. "Data flow into
16 system accomplished by various USB flash drives -
17 not encrypted, not serialized - so no ability to
18 track full lifecycle and pinpoint data loss."

19 Do you see that?

20 A. Yeah. They actually are encrypted, but
21 they were not serialized.

22 Q. And so data was brought into the EMS
23 system through these USB drives; is that correct?

24 MR. MILLER: Objection. Lack of
25 foundation.

THE WITNESS: I think we probably ought to ask Michael Barnes about that.

I believe that the markups came back on the USB drives. I'm not sure the markups ever made it back to EMS.

I think the idea is is you look at somebody's markups and then they go back into the EMS system and make those changes. I don't think the file itself actually got pushed back into the EMS.

Think of it as a poor man's markup language. And sometimes in some of the counties, it was a -- it was a, you know, photograph of the ballot with pen marks of what they wanted moved, things like that.

So, yeah, I don't -- that doesn't have any systematic value to the system, so it would be a -- one of Michael Barnes' folks that would do that. But, again, I'd verify it with Michael Barnes.

BY MS. KAISER:

Q. And further down -- or, sorry, the next page under "Other," the second bullet point there, "Liked the idea of leaving the legacy system [sic] alone, spinning up a second VM host for new

Page 131

1 applications - allowing the other to be idled in
2 place for retention without impact."

3 Do you see that?

4 A. Right. Yeah.

5 Q. And, again, that --

6 A. That's --

7 Q. -- was your recommendation?

8 A. That was -- that's known as
9 shrink-wrapping, right? In other words, we don't
10 want to mess with the source system. We derack it
11 with all the data on it, we wrap it up in shrink
12 wrap, and we secure it in a location. That way it
13 can always be referenced in its original form.

14 Q. And the next bullet says, "No need to have
15 connectivity between old and new - as the data is
16 moved 'sneakernet' or equivalent."

17 A. Right.

18 Q. What does "sneakernet" mean?

19 A. Just a manual process, no electronic link,
20 no Ethernet. You know, it's just moving it by
21 person.

22 Q. And you said that this recommendation to
23 spin up a new server was -- was accepted and that's
24 what ultimately --

25 A. Yes --

Page 132

1 Q. -- happened; is that right?

2 A. -- yes, yes. They didn't have a choice.

3 They had to -- to run the newest code, they had to
4 have a newer version of processors, right.

5 Q. And I think we mentioned the term "air
6 gapped."

7 What do you understand the term "air
8 gapped" to mean?

9 A. Not connected to the open public Internet
10 in any way.

11 Q. And so is the new server that houses the
12 EMS system supposed to be air gapped?

13 A. It is.

14 Q. And why is it important for that server to
15 be air gapped?

16 A. There was a policy at some point that they
17 decided -- and this, again, is memory -- so it was
18 always air gapped, so we wanted to retain that -- I
19 don't like using the term "air gapped," but,
20 basically, it was disconnected from the Internet,
21 never to be connected to the Internet.

22 Some air-gapped systems are air gapped
23 partially and then when it comes time for updates,
24 they plug it in. That's not the case here. There
25 was no way into that system from the Internet.

1 Q. That was my next question.

2 So to your knowledge, this system was air
3 gapped?

4 A. Correct.

5 Q. And to ensure that this -- that the EMS is
6 air gapped, it would have to be completely detached
7 or disconnected from other parts of the IT
8 infrastructure in the Secretary of State's office
9 that does connect to the Internet; is that right?

10 A. Correct.

11 MR. MILLER: Object to the form of the
12 question. Compound.

13 BY MS. KAISER:

14 Q. And to your knowledge, that's the case
15 that --

16 A. It is --

17 Q. -- this --

18 A. -- the case, yeah, yeah.

19 Q. Are there any components of the BMD system
20 that are connected to the Internet?

21 A. "BMD" meaning the -- the Michael Barnes
22 environment that does the ballots?

23 Q. Yes.

24 A. No. They have a separate desktop on each
25 one of the users, and that's the desktop that they

Page 134

1 use to connect to it.

2 Then they have another desktop that's for
3 their normal use. There's no email, there's no
4 anything on the other one except the application.
5 It runs on a separate physical network all the way
6 to the wires -- all the way to the wires, all the
7 way back. So...

8 MS. KAISER: Let's load Tab 11, please.

9 THE WITNESS: Did you say 11? I'm sorry.

10 (Plaintiffs' Exhibit 15 was marked for
11 identification.)

12 BY MS. KAISER:

13 Q. I'm sorry. That -- that was Tab 11 for us
14 internally.

15 A. Oh, okay.

16 Q. Exhibit 15.

17 A. Okay.

18 Q. It should be up now.

19 So you'll see this starts with an email
20 from Frances Watson on October 29, 2020.

21 A. Uh-huh.

22 Q. Do you see that?

23 A. I remember, right.

24 Q. Who is Frances -- who is Frances Watson?

25 A. She's the chief investigator for the

Page 135

1 Secretary of State, the organization. She's a --

2 Q. So did you work with her?

3 A. Yeah. She's a sworn law enforcement
4 agent. So...

5 Q. And you said you remember. What do you
6 remember about this incident?

7 A. Just that the county that had this
8 problem -- basically, my memory is is that someone,
9 a poll worker, said, "Hey, my mouse is moving and
10 I'm -- I'm not doing it. It's like somebody has
11 remote control of my system."

12 So one of the poll supervisors, of course,
13 shut the notebook down, completely disconnected it,
14 and it became kind of a thing. And we heard about
15 it through the County and they wanted us to help
16 with it to make sure that there wasn't anything
17 nefarious going around.

18 So we had Frances Watson's organization
19 take possession of that and send it directly to
20 Fortalice to have it analyzed to see if there's
21 any -- anything on it that might be, you know,
22 malware, keyloggers, that kind of stuff. We sent it
23 directly to -- to their folks. I think
24 Chris Furtick was in that group.

25 So, anyway, we never touched the notebook

Page 136

1 because we wanted to maintain the chain of custody.
2 But they didn't find anything out of the -- out of
3 the norm, so eventually it was returned to Fulton
4 County by Frances and her organization.

5 Q. If you look at the -- let's see -- page 3,
6 there's an email from Adrick Hall on October 29th.

7 Do you see that?

8 A. Page 3. Let's see. Got it.

9 Q. It's the page ending --

10 A. Got it.

11 Q. -- in -1211.

12 A. Okay. I got it. The one that starts
13 "Braun is here [sic]"?

14 Q. Yes.

15 A. Okay.

16 Q. About three lines in, it says, "The
17 general statement is that the laptop was a Fulton
18 County laptop. The" -- I think maybe it's "they" --
19 "used it to access ElectioNet and Easy Vote and
20 process the AB applications for voters."

21 Do you see that?

22 A. Right. Absentee --

23 Q. So this election --

24 A. -- ballot.

25 Q. -- this laptop -- I'm sorry. What was

1 that?

2 A. The "AB" is absentee ballot. Right.

3 Q. All right. So the laptop was being used
4 to access ElectionNet and Easy Vote and to process
5 absentee ballots; is that correct?

6 A. Sounds like it, yep.

7 Q. Okay. And it says, "The laptop was on
8 Wi-Fi mode and the cursor began to move from icon to
9 icon on its own."

10 Do you see that?

11 A. Yes.

12 Q. Was it consistent with policy for that
13 laptop to be in Wi-Fi mode?

14 MR. MILLER: Objection. Lack of
15 foundation.

16 THE WITNESS: I can't -- can't speak for
17 the counties, the individual counties.

18 BY MS. KAISER:

19 Q. Okay. Would it be -- based on your
20 experience and training, would that -- would that be
21 best -- a security best practice, to have a laptop
22 that was being used for these purposes connected to
23 the -- to Wi-Fi?

24 MR. MILLER: Same objection. Lack of
25 foundation.

Page 138

1 THE WITNESS: Yeah, just from an -- an
2 opinion base, it all depends on the
3 circumstances and what their wireless network
4 looks like.

5 I mean, I've got a huge wireless network
6 at the hospital that I feel very confident
7 about its security, so I don't have any problem
8 with PHI running left and right.

9 But I just don't know enough about their
10 network to make that call.

11 BY MS. KAISER:

12 Q. And when -- a laptop like this that was
13 used by Fulton County -- a poll worker in Fulton
14 County, would that have any connectivity to the EMS
15 system that we would -- were talking about
16 previously?

17 A. No.

18 MR. MILLER: Foundation.

19 BY MS. KAISER:

20 Q. So moving up in the document, you see the
21 bottom of page 2 an email from Ryan Germany, "Should
22 we have Fortalice or someone do some forensics on
23 this laptop?"

24 You said that is what happened?

25 A. That is what happened, right.

Page 139

1 Q. And Fortalice determined there was no
2 malware or --

3 A. No.

4 Q. -- something similar on the laptop?

5 Do you know what permissions are required
6 to access the EMS server?

7 A. Are we talking about the ballot
8 development server?

9 Q. Yes.

10 A. Yeah, you have to have an independent
11 account on that environment, a named account. There
12 are no -- there are no generic users. Password
13 complexity --

14 Q. There's no -- please. Sorry. Go ahead.

15 A. Yeah, it has password complexity and --
16 and some other things that just harden that side of
17 the house.

18 Q. Are there any full-admin permissions for
19 that server?

20 MR. MILLER: Objection --

21 THE WITNESS: Yes.

22 MR. MILLER: -- lack of foundation.

23 COURT REPORTER: Repeat the objection,
24 please.

25 MR. MILLER: Lack of foundation.

Page 140

1 COURT REPORTER: Thank you.

2 One at a time, please.

3 BY MS. KAISER:

4 Q. And how do you know that, that there are
5 full-admin permissions for that server?

6 A. Because you'd have to have it to install
7 software, so the IT group had administrative access
8 to it to be able to maintain it.

9 Q. Did anybody else have access?

10 A. Just the IT group, right.

11 MR. MILLER: Hey, Mary, when you get to a
12 good point, if we could take a break for a
13 quick second.

14 MS. KAISER: Yeah. This is a good time.

15 MR. MILLER: Not right this second, but up
16 to you.

17 MS. KAISER: No, this is a good time.

18 We're moving to a different topic.

19 So -- and I don't know, Mr. Hamilton, do
20 you -- do you want to take a quick lunch break?
21 I know it's the middle of the day. So...

22 THE WITNESS: No, we're good. We can --
23 if you guys are okay, I can go through. That's
24 fine.

25 MR. MILLER: We --

Page 141

1 MS. KAISER: Okay. Do you want to just
2 take a -- sorry, Carey.

3 MR. MILLER: Yeah. How much are you
4 anticipating going forward? We can talk about
5 this --

6 MS. KAISER: I'd say --

7 MR. MILLER: -- off the record.

8 MS. KAISER: Yeah, I'm sorry. Let's go
9 off the record.

10 VIDEOGRAPHER: The time is 1:03. We're
11 off the record.

12 (Off the record.)

13 VIDEOGRAPHER: The time is 1:17. We're
14 back on the record.

15 BY MS. KAISER:

16 Q. Mr. Hamilton, I think we've discussed
17 ElectionNet several times. I just wanted to ask a
18 few more questions about that.

19 So can you just describe generally what
20 ElectionNet is?

21 A. It's just a voter registration system. It
22 allows the public to register for -- to vote, to
23 check what precinct they vote in, that kind of
24 stuff. Kind of a --

25 Q. Does it store voter information?

Page 142

1 A. Address, some -- some PII, but not -- not
2 the extent that would rise to the level of driver's
3 license, license numbers, things like that. It's
4 just normally public-facing information.

5 Q. Do you know how that information is used
6 in Georgia elections?

7 A. Well, they -- I know they make it
8 available to anybody that, you know, runs or has
9 interest in it. For a fee, they sell the file. You
10 know, that -- that happens pretty normally as a
11 normal course of business.

12 Q. And do you have any understanding about
13 how the voter identification data in ElectioNet
14 is -- is used with, for example, poll books?

15 A. No. Just that the -- the poll books were
16 supposed to be a -- a backup to them. Maybe not as
17 timely as -- as -- as the electronic form, but the
18 poll books are printed a few days before the
19 election. And that's to be used in emergency if for
20 some reason ElectioNet goes down or something like
21 that. But it's -- I believe it's the same
22 information.

23 Q. Are you aware that in August of 2019, the
24 judge in this case ordered the Secretary of State's
25 office to conduct a cyber- -- cybersecurity

1 assessment of the ElectionNet database?

2 A. I -- I remember, yes.

3 Q. And did that review ever happen?

4 A. Yeah. That was done by -- by Fortalice.

5 Q. And do you know what Fortalice found as
6 part of that assessment?

7 A. I don't have the report right with me, but
8 there was a special carve-out for just those two
9 systems.

10 Q. Do you recall generally what the Fortalice
11 report found with respect to the systems?

12 A. I don't believe there's any criticals.

13 There might be a high or two. Most of them were
14 medium.

15 Mediums are pretty prevalent in any
16 system. We try to hit off the highs and especially
17 criticals. Criticals we'll stop the presses for and
18 try to at least -- remediate them or at least, you
19 know, put some parameters around it or a
20 compensating control to reduce the threat. So...

21 Q. And do you know what steps have been taken
22 to remediate any of the vulnerabilities identified
23 by Fortalice in that report?

24 A. No, not without seeing the report. Then I
25 can speak to each one. But...

Page 144

1 Q. What office or entity has responsibility
2 for ElectioNet currently, do you know?

3 A. Secretary of State. That's one of the
4 three --

5 Q. And is it your --

6 A. -- pillars. Sorry.

7 Q. Is it your understanding that PCC
8 previously owned and operated ElectioNet?

9 A. Yes.

10 Q. But the Secretary of State's office has
11 taken over ElectioNet?

12 A. Correct.

13 MS. KAISER: If we could look at Tab 24,
14 please.

15 (Plaintiffs' Exhibit 16 was marked for
16 identification.)

17 BY MS. KAISER:

18 Q. It should be Exhibit 16.

19 A. Okay. Got it.

20 Q. Do you recognize this document?

21 A. Yes. This was the second one I did.

22 Q. The second declaration?

23 A. (Nodded head.)

24 Q. Okay. See in paragraph 12 of this
25 declaration, the last sentence there on page 9?

Page 145

1 A. Oop, I went past it.

2 Q. It says, "To be clear, the P-" -- oh,
3 sorry.

4 A. Got it. I got you.

5 Q. "To be clear, the PCC environment was
6 transitioned to full SOS control and responsibility
7 as of July 2019."

8 Do you see that?

9 A. Okay. Apparently I was not on the --

10 Q. What is the --

11 A. -- right page.

12 Q. -- "PCC environment"? Oh, sorry.

13 A. Sorry. I guess it was -- you really meant
14 page 9. I was looking at Bullet 9. So...

15 Q. Oh, yeah, page 9 --

16 A. Okay. Got it.

17 Q. -- paragraph 12 --

18 A. Yeah.

19 Q. -- last sentence there.

20 A. Uh-huh. Yep.

21 Q. Okay. What is the "PCC environment"?

22 A. That was the ENET, the corporation side,
23 everything that they did for us. They -- and as I
24 understand it, they used to -- they -- the original
25 contract was kind of an all-in, you know, they are

Page 146

1 responsible for the -- running the servers and
2 patching and doing all the operational things that a
3 normal IT organization would do as a service.

4 And I think because of the shortfall of
5 that service and some -- the decision was made to
6 bring that back -- even though the hardware was
7 actually owned by the State, the decision was made
8 to bring that back under the control of -- of the
9 infrastructure through -- at Secretary of State,
10 which was Bill Warwick and Jason Matthews, those two
11 guys.

12 Q. And forgive me, I don't recall. Did
13 you -- did you testify that you were part of that
14 decision?

15 A. No, I'm not a part of that decision. I --
16 I -- my -- I think it was a good idea, but the -- I
17 don't believe I -- I had a hand in that.

18 I think part of my engagement there was to
19 evaluate a replacement data center, and the move to
20 QTS was on my recommendation -- that was away from
21 the -- the White Street Zayo facility that they were
22 in -- for no other reason than just get some
23 distance from -- from the other hosted systems that
24 they had there.

25 Q. And when you said in your declaration that

Page 147

1 it was tran- -- the PCC environment was transitioned
2 to full SOS control and responsibility, what did you
3 mean by that?

4 A. For patching, the normal care and treating
5 of a server, making sure that, you know, we could
6 get to it, administrative control.

7 We were able to -- to lock a -- all the
8 PCC folks out of it unless they absolutely needed
9 access, and then it was only on a temporary basis.
10 So by "control," it's just that administrative
11 control, knowing, you know, what levels of patches
12 are there and things like that.

13 And I -- I believe they --

14 Q. Do you --

15 A. -- struck a new contract with the
16 provider.

17 Because PCC had the original contract and
18 had other states' information and other customers
19 kind of in that rack commingled. So the idea of us
20 breaking away from them, we had to physically move
21 them to a separate rack to be on our own. I think
22 that took us to strike our own contract with -- with
23 Zayo.

24 And that was a temporary move --

25 Q. When you say "rack" --

Page 148

1 A. A rack -- it's an empty -- it's an empty
2 metal cabinet that you actually slide the servers
3 into. Allows air -- free air flow. There's a
4 power -- A and B power so you can have a power
5 outage and not stop the world. It's a service that
6 data center providers provide. You can buy a rack
7 from somebody.

8 Q. As of July 2019, is it accurate that PCC
9 no longer had any responsibility for hosting or
10 managing ElectioNet?

11 A. Other than the application that rides on
12 it, no. From the -- from the patching and
13 day-to-day care and feeding of it, it was -- it was
14 our guys.

15 Q. What steps did the Secretary of State's
16 office take to remediate the -- the known security
17 vulnerabilities that were present in ElectioNet
18 after taking control of it?

19 MR. MILLER: Objection. Misstates
20 testimony not in evidence.

21 THE WITNESS: Just that they worked --
22 continued to work the same list.

23 Some of it made -- it made it a lot easier
24 on us because we were able to see into the
25 environment, where we hadn't been able to see

Page 149

1 before as a user, right? So we were able to
2 fix a lot of things even not captured in other
3 reports that we felt needed to be done.

4 MS. KAISER: Tab 13, please.

5 (Plaintiffs' Exhibit 17 was marked for
6 identification.)

7 THE WITNESS: 17?

8 BY MS. KAISER:

9 Q. Yes.

10 Have you had a minute to review the
11 document, Mr. Hamilton?

12 A. I got it. Yep.

13 Q. So this is an email chain from April of
14 2019 with the subject "Fannin County IP."

15 Do you see that?

16 A. Uh-huh. Got it.

17 Q. Do you remember the incident that's being
18 described in this document?

19 A. Not particularly, no.

20 Q. So we'll walk through this.

21 So the first email in the chain looks like
22 it has -- just contains a series of numbers that
23 looks like --

24 A. An IP address.

25 Q. -- an IP address.

1 A. Correct.

2 Q. And then if you go up in the email, it
3 says, "This is one of several blocks from this
4 morning."

5 Do you see that?

6 A. Yes.

7 Q. And so it looks like, you know, what was
8 happening here is that this IP address from --
9 allegedly from Fannin County was blocked.

10 A. Correct.

11 Q. Is that your understanding?

12 A. Uh-huh.

13 Q. So if you look on page 1 of the document,
14 Clark Rainer's email at the bottom of page 1 --

15 A. Right.

16 Q. -- it says, "We have a web application
17 firewall running on the Voter Registration --
18 Georgia Voter Registration System, and this is the
19 system the elections offices use [sic] to update
20 voter records."

21 Do you see that?

22 A. I do.

23 Q. So was that the ElectionNet system that
24 he's describing?

25 A. Part of it, right.

Page 151

1 Q. Okay. And then he goes on to say that
2 they've identified the IP address and it's been
3 blocked.

4 Do you see that series of four bullet
5 points?

6 A. Correct.

7 Q. "Just got an email from MS-ISAC with some
8 more information I'll forward on in just a minute
9 also showing you may have a malware infection."

10 Do you see that?

11 A. I do.

12 Q. Do you recall whether there was any
13 investigation into whether this was a malware
14 infection?

15 A. I do not. Not specific to Fannin County,
16 no. This -- this would have been a normal
17 occurrence, though, from the firewall. That's what
18 its job is to do, is to actively block anything that
19 it thinks is -- in this case, it appeared like a
20 false positive because it was coming from a county.

21 But because of the way it was flagged, we
22 were just being a good community member and letting
23 them know, "Hey, you might have a malware thing, so
24 heads up."

25 Q. And, yeah, I mean, I was -- I was going to

Page 152

1 ask if there was any investigation done to determine
2 whether this was actually coming from the County,
3 this IP address.

4 A. Yeah, I think that would be on the County.
5 I think Clark sending up a flare and saying, "Hey,
6 we have this" -- I'm sure this originally came from
7 the people in Fannin County saying, "Hey, we can't
8 get into the election system this morning." And
9 that would have been on purpose because the firewall
10 would have clamped them.

11 So -- but I do not remember this
12 specifically. It didn't trigger an incident
13 response that I can recall. So...

14 Q. We're adding Exhibit 18 now, Mr. Hamilton.

15 (Plaintiffs' Exhibit 18 was marked for
16 identification.)

17 THE WITNESS: 18. Okay. I got it.

18 BY MS. KAISER:

19 Q. All right. This is an email chain, see,
20 from October -- sorry -- let's see -- starts in
21 July 2020.

22 Do you see that?

23 A. I do.

24 Q. And the first email in the chain is from
25 you to Ashwin Ramaswami.

1 Do you see that?

2 A. Uh-huh. Right.

3 Q. Who is -- who is Ashwin Ramaswami?

4 A. He worked for -- I'm sorry, he was a
5 student at Stanford. This is one of those
6 John Q Public heads up from the -- from the world,
7 because he didn't obfuscate his -- you know, his --
8 didn't make a big deal of "I want to stay private,"
9 everything else.

10 So this is basically a conversation that I
11 forwarded on that I had with this -- I believe this
12 went originally to one of the leadership. I'm
13 not -- it didn't come to me. Somebody -- somebody
14 said, "Hey, check out this email address" or -- I
15 don't know how we originally found this.

16 But, yeah, Ashwin is the -- is the student
17 who, at that point, claimed to be a Georgia
18 resident. His dad lives in Johns Creek, which is
19 around the corner. Had a lot of information about
20 that.

21 And, actually, in other conversations,
22 found that we had a common thread through somebody I
23 used to work for -- or worked with 10, 15 years ago.
24 So it didn't look like it was bogus, so that's why I
25 kind of ran it down.

Page 154

1 Q. Okay. Yeah. So in this first email, you
2 say, "Ashwin, Thanks again for your email regarding
3 MVP, the vendor is currently working to validate,
4 recode and test those issues you identified."

5 Do you see that?

6 A. Correct. Correct.

7 Q. Do you recall what issues Mr. Ramaswami
8 identified with MVP?

9 A. No, not right offhand. I think some of it
10 was SQL -- SQL injection maybe or cross-site
11 scripting. It wasn't something super deep, because
12 they were able to remediate it pretty fast.

13 Q. But it was a valid vulnerability?

14 A. Yeah.

15 The second -- the second thing he sent me
16 was about what appeared to be the source code for
17 our ElectioNet system on a publicly available
18 website. That's the GitHub.

19 Q. Right.

20 A. Yeah.

21 Q. Right. I think if you go up two emails --
22 let's see -- at the top of the next page, there's an
23 email from Mr. Ramaswami on October 16.

24 A. Right.

25 Q. And he said, "Wanted to let you know about

Page 155

1 another issue: It seems like the Georgia --
2 Georgia's ElectionNet system's source code is
3 available publicly in GitHub."

4 Do you see that?

5 A. Correct. Yep.

6 Q. And that's what you were just referring
7 to?

8 A. Correct.

9 Q. Okay. So what is GitHub?

10 A. GitHub is a -- is a sharing platform,
11 basically, for programmers. If you can -- I -- we
12 talked about a Wiki before. It's sort of kind of
13 like that.

14 Folks -- programmers will go out there
15 and -- and kind of copy snippets of code so they
16 don't have to write it from scratch. So you piece
17 things together using libraries and things like
18 that. It's just a community of software developers,
19 but it's a worldwide thing.

20 So there's, you know, source code on there
21 for Windows and all kinds of strange stuff. So...

22 Q. So Mr. Ramaswami was alerting you to the
23 fact that source code for Georgia's voter
24 registration system was posted on a public website;
25 is that right?

Page 156

1 A. Correct.

2 Q. And he says in the next line, "The [sic]
3 repository also appears to contain passwords and
4 private keys."

5 A. Correct.

6 Q. Do you see that?

7 A. Right.

8 Q. What was the significance of that?

9 A. The passwords ended up being test accounts
10 that -- that software -- this source code came from.

11 The private keys also were to test
12 instances, not the production side, so there wasn't
13 direct involvement of the production code line.

14 But in further investigations, what this
15 was was a programmer that worked for PCC posting it
16 there because it was easier than copying it
17 somewhere else. I don't know what the excuse was.

18 But we came down kind of hard on PCC about
19 that and they rectified it, I think, within 24
20 hours. I mean, I think they pulled it down.

21 And GitHub does a pretty good job of
22 logging access instances and also instances where
23 folks that had actually taken a snippet or
24 downloaded the code.

25 And PCC was able to verify and

Page 157

1 authenticate that all of the accesses to that code
2 line with the exception of me and one other guy from
3 the SOS that were just checking it out were, in
4 fact, PCC employees. So...

5 Q. So you forwarded Mr. Ramaswami's email to
6 a couple of folks at Fortalice; is that right?

7 A. Right.

8 Q. And asked -- and asked them to look into
9 it?

10 A. Correct. Right. Because they've got --

11 Q. So that's the --

12 A. -- application -- I'm sorry.

13 Fortalice has application-specific talent
14 that understands code lines, programming, all that
15 good stuff, and they probably frequent those
16 libraries and frequent that site. So that was the
17 best place to go, because the SOS organization had
18 no programmers.

19 So that was my idea, is to involve them
20 early to see what -- this thing and how it panned
21 out.

22 Q. And so working with Fortalice, that's how
23 you determined that -- that this was put on GitHub
24 by a programmer for PCC; is that right?

25 A. Well, they -- they were able to come up

with the IP addresses of -- of people that had accessed the library. And further investigation and once I supplied those to PCC, they were able to validate each one of those IP addresses were their employees. So...

6 Q. And so the -- the -- what was done to
7 remedy this was just to have PCC pull the --

A. Yeah, to destroy it.

9 Q. -- pull the --

A. Yeah, to pull it down, right.

11 Q. Was anything else done to remediate this
12 incident?

13 A. No. I think -- I -- I know that there
14 were some phone calls that I was not involved in
15 between leadership and SOS and PCC. I'm sure they
16 were not comfortable phone calls, because they were
17 getting -- you know, it was just -- but I wasn't
18 part of the phone call, so that's a Merritt
19 question.

Q. We're going to look at the next exhibit.
I believe it's Exhibit 19.

24 THE WITNESS: Okay. I got it. That's a
25 wicked pattern.

Page 159

1 BY MS. KAISER:

2 Q. This is --

3 A. Okay.

4 Q. This is a report from Fortalice Solutions.

5 Do you see that?

6 A. Yes.

7 Q. Dated July 14, 2020?

8 A. Right.

9 Q. If you look at page 2 of the report --
10 it's the third page of the document, but it says
11 page 2 at the bottom --

12 A. Okay.

13 Q. -- under Section 1.1, "Overview," it says,
14 "In June of 2020, Secretary of State Georgia
15 received report of two vulnerabilities in a web
16 application hosted at
17 [https://www\[.\]mvp\[.\]sos\[.\]ga\[.\]gov](https://www[.]mvp[.]sos[.]ga[.]gov)."

18 Do you see that?

19 A. Correct. Yep.

20 Q. All right. So this is -- the "MVP" is the
21 My Voter Page; is that right?

22 A. Yes.

23 Q. And the next sentence says, "Upon
24 attempted remediation, SoSGA requested that
25 Fortalice validate the remediation attempts."

1 Do you see that?

2 A. I do.

3 Q. Do you recall anything about this
4 incident, about --

5 A. Yeah. Basically --

6 (Cross-talk.)

7 A. Basically, we were asking Fortalice to
8 verify what we were being told by PCC as "it's
9 fixed." Because we didn't have the -- the
10 wherewithal to, you know, go through this stem by
11 stem, we got Fortalice to do it as a third -- third
12 party. So...

13 Q. And what did Fortalice find?

14 A. They found that actually they had not
15 remediated it sufficiently, and they made a
16 suggestion on how to fix it the right way. And we
17 fed that information back to PCC.

18 0. This is in 2020; correct?

19 A. Probably. Yeah.

20 Q. Did PCC still have responsibility for the
21 MVP page in 2020?

22 A. No.

23 Q. So why did you need to feed the fix back
24 to PCC?

A. Because they still write the code. They

Page 161

1 still manage the application, they just don't manage
2 the hardware. So they're still responsible for the
3 code line.

4 Q. So when you identified a vulnerability on
5 the My Voter Page, you still had to rely on PCC to
6 fix it?

7 A. Correct.

8 Q. If you look at page 4 of the Fortalice
9 report --

10 A. Okay.

11 Q. -- under "Conclusion," it says, "The
12 remediation attempts that are currently in place
13 partially fix the issues in the original report, but
14 more work needs to be done to secure the website
15 from potential attacks."

16 Do you see that?

17 A. Right.

18 Q. "In addition to the checks performed,
19 Fortalice noticed other areas of potential impact
20 that, while unconfirmed, Fortalice believes could be
21 used to further exploit the site or the servers
22 hosting it. Fortalice recommends having the
23 application thoroughly reviewed for similar issues."

24 Do you see that?

25 A. Correct. Right.

Page 162

1 Q. Do you know whether that recommendation
2 was accepted, to have the application reviewed for
3 similar issues?

4 A. I -- I didn't. I didn't have an
5 application-specific review done for them because
6 I -- I think at that point, the decision had been
7 made to jettison PCC.

8 So I think leadership looked at it as,
9 "We're going away from them, so, you know, we're
10 going to spend the time on the new stuff."

11 We did feed all this information back to
12 them, that there might be some other areas and, you
13 know, as a partner, we expect them to, you know,
14 find some of their own issues. We don't want to
15 be -- be their QA group. So...

16 Q. I just want to make sure I understand the
17 timing, because, you know, I -- I've understood you
18 to say that PCC was jettisoned in 2019; is that
19 right?

20 A. From the operational standpoint, right,
21 the care and feeding of the servers, the patching,
22 that kind of stuff, and the contract of housing the
23 servers and we're paying them to do that service.

24 But the actual code line, the development
25 and the -- and the -- you know, the changes that

Page 163

1 were made to MVP and all those -- OLVR, all those
2 systems, were still under their control because they
3 were the developers.

4 Q. Right.

5 And so by 2020, the Secretary of State's
6 office had taken over with respect to the security
7 of these applications; is that right?

8 A. Well, insofar as we can handle it from
9 the -- from the edge. But as far as internal to the
10 actual application, we still have to rely on PCC to
11 do what they profess they're experts at.

12 So that's why we run these monthly checks,
13 and what we do with Fortalice with pen tests is to,
14 you know, trust but verify, right? We verify what
15 they told us to be true.

16 Because the Secretary of State doesn't
17 employ any developers, that's -- that's a bit of
18 a -- a hill to climb. We didn't have anybody in
19 there that wrote code, so we couldn't really
20 challenge them on a code line level. We just
21 identified, "Hey, this doesn't work right; go fix
22 it."

23 Q. So when --

24 A. This --

25 Q. -- Fortalice recommended -- recommended a

1 thorough application review, is that --

2 A. Uh-huh.

3 Q. -- something that the Secretary of State's
4 office could carry out, or would you have to rely on
5 PCC?

6 A. No, no, no. We would have to actually
7 hire another company to do that as a third party.

8 So they would take the source code, they
9 would go review the source code and how the program
10 is written, and make recommendations, look at common
11 security vulnerabilities.

12 There's a term "OWASP." It's for the --
13 you know, the top 25 things that people do wrong in
14 programs. And they were missing some of the basic
15 stuff, so we started beating up on them about being
16 at least OWASP compliant.

17 But it would have been a third party. I'm
18 not sure if -- if Fortalice provided that. They --
19 they may or may not have had that as -- it sounds
20 like it is. It sounds like, "Oh, by the way, you
21 know, we could do this for you," cha-ching, you
22 know, that kind of thing.

23 Q. But to your knowledge, that kind of
24 thorough review of the application for similar
25 issues to the ones you identified at the time was

Page 165

1 never done?

2 A. Not while I was there. It might have been
3 done after I left, but, again, that's --

4 Q. You're not aware of that?

5 A. I'm not aware of it, right.

6 MS. KAISER: Tab 18, please. I'm adding
7 Exhibit 20.

8 THE WITNESS: Okay.

9 (Plaintiffs' Exhibit 20 was marked for
10 identification.)

11 THE WITNESS: Okay.

12 BY MS. KAISER:

13 Q. This is an email from you dated April 29,
14 2021.

15 A. Right.

16 Q. Do you see that?

17 And it says to Ronnell Spearman, Derek
18 Hawkins, and DeVon King.

19 A. Right.

20 Q. And are those -- are those the three
21 security analysts that reported to you --

22 A. At that --

23 Q. -- at this time?

24 A. -- time, right.

25 COURT REPORTER: One at a time, please.

1 THE WITNESS: DeVon King replaced one of
2 the guys, right.

3 BY MS. KAISER:

4 Q. You say, "My latest response to
5 KRob - ok - understood."

6 And is "KRob" Kevin Robertson?

7 A. Kevin Robertson, yeah. That was his
8 nickname because we had too many Kevins.

9 Q. You say, "I would like to know are these
10 two apps on different physical db servers or
11 different instances on the same?"

12 Do you see that?

13 A. Yep.

14 Q. Do you know what apps you were talking
15 about in this email?

16 A. Not without seeing the -- the response
17 that I sent to KRob. If you have that email, I
18 could probably tell you.

19 They were pretty good about segmenting the
20 databases away from each other on different
21 instances, because they wanted to keep them
22 physically and logically separate. But it all
23 depends on what we were talking about.

24 "Secure tunnel," that's a way of
25 transmitting over the open Internet. Yeah.

1 Enabling TLS.

2 Q. Yeah.

3 A. Right.

4 Q. We were -- we were trying to figure out
5 what this email was -- was referring to in terms of
6 the two apps.

7 A. Yeah, it's -- if you had the --

8 Q. Let me just --

9 A. If you had the other email, it would
10 probably help me kind of weed this one down.

11 But these are -- this is generic things
12 that I asked my team to go hunt down on different --
13 it's basically you're -- we're looking for the --
14 how -- how hardened the simple -- a simple site is,
15 right, what -- what did they -- how far did they go
16 to make things encrypted and safe.

17 And I mention there that I know that with
18 self-signed certs, sometimes that breaks the app,
19 but it's better than nothing.

20 Well, and the intent there is that there
21 is -- and this is industry-wide, not just the
22 State -- but there is a -- kind of a rub between
23 development and operations. You know, they -- they
24 point at each other for the fault of things.

25 A lot of times developers will say, "No,

1 you can't take that patch. You can't update that
2 server because you're going to break the app."

3 And this is my response to it.

4 Apparently, I was saying, "Yeah, I understand that
5 it might break the app, but we gotta do something,"
6 right? So this is -- sounds like a conversation
7 around a compensating control.

8 Q. And a compensating control means something
9 you would do to remediate a vulnerability you've
10 identified?

11 A. Correct. And that -- the idea is that
12 there's more than one way to -- to address a
13 problem.

14 And mitigation is a -- is only a snapshot
15 in time, so we do -- we do mitigations. We do
16 compensating controls when we can't fully mitigate.
17 Like I said, when a developer tells you, "You can't
18 do that, you'll break the app," we do other things
19 to protect the house. So...

20 Q. And the last line of this email, you say,
21 "All connections" -- "ALL" in caps --

22 A. Right.

23 Q. -- "All connections internal should be
24 encrypted and we ought not use the standard 1433
25 port."

1 A. Correct.

2 Q. Do you see that?

3 A. Right. So internally to the SOS, what I
4 was talking about there is that the actual
5 connections that are made between the application
6 servers, which service the front end -- like when
7 you're typing in My Voter Page, you're running a
8 program on those servers -- there is a secure link
9 that goes from that server through the covers to the
10 actual database server itself. And that is on Port
11 1433. Normal- -- normally, you can make the port
12 anything you want.

13 The idea of changing from the -- from the
14 regular port number is just a way to obfuscate what
15 that traffic might be. Because it's encrypted, it
16 would be very hard for an outsider or, you know,
17 even somebody from the inside to be able to sniff
18 the traffic and figure out what it is.

19 So that's just a good practice, that
20 even -- people think of it like a -- a castle with a
21 moat, right? We only worry about the Internet.

22 But internal to the system, as a -- as an
23 organization moves through that maturity of
24 security, you -- you move more towards a zero trust.
25 I don't know if you've heard that term before. And

Page 170

1 the idea is you treat internal assets as if they
2 were public, and that helps harden things.

3 And that -- this is basically me kind of
4 coaching my guys about, "Go look at this stuff and,
5 oh, by the way, you know, think long term. All of
6 our internal connections need to be fully encrypted
7 and we ought to not use standard ports, because it
8 just makes it easy for the bad actors." So that was
9 what that was about.

10 But specific to each individual point, I
11 would imagine if we had the original email that I
12 sent to KRob, I could probably speak to it.

13 Q. You say, "...ALL connections should be
14 encrypted...."

15 To your knowledge, were all internal
16 connections encrypted?

17 A. Not at that point. There were -- to the
18 database servers they were, but there was other
19 applications not affiliated with the ElectioNet, but
20 there was other applications internal to the -- to
21 the SOS that just had public information and they
22 didn't deem it.

23 But it's -- easier from a security
24 perspective is to make everything standard. That
25 way if anything falls out of the bucket, it's easy

Page 171

1 to identify. I don't want to have to pick and
2 choose.

3 That's why I was telling him about the
4 long term, get everything under the same hat.
5 Regardless whether it's public information or not, I
6 don't care. I still want to encrypt it internally.
7 So -- it doesn't cost any more; it's just coding it
8 that way. So...

9 Q. Are you aware of what operating system
10 Dominion's BMD machines runs on?

11 A. No.

12 MS. KAISER: Tab 20, please.

13 THE WITNESS: Yeah, the -- the ballot --
14 the ballot situation over at EC is running on
15 Windows Servers, but they're in virtual
16 machines. So -- but I know --

17 BY MS. KAISER:

18 Q. I meant the BMD.

19 A. Okay. All right. Yeah, that -- I'm
20 sorry. I had it in my mind that you were talking
21 about the poll pads and all that stuff.

22 Yeah, those are -- those Windows --
23 Windows Server.

24 Q. Right. No, I was talking about the BMDs
25 themselves, not --

1 A. Oh.

2 Q. -- not the EMS server.

3 A. Okay. I guess -- I guess I need a
4 clarification.

5 BMD's not a term -- is this the ballot
6 system again, or are we talking about --

7 Q. Yes. I'm sorry. No, the -- the
8 ballot-marking devices, the devices themselves, the
9 machines.

10 A. Yeah, and I don't -- I -- I've never
11 looked under the covers over there.

12 Q. Okay. Understood.

13 (Plaintiffs' Exhibit 21 was marked for
14 identification.)

15 (Plaintiffs' Exhibit 23 was marked for
16 identification.)

17 MS. KAISER: Okay. Let's see. We've
18 added Exhibit 21, I think. Is that -- okay.
19 Pull that up.

20 THE WITNESS: Okay.

21 BY MS. KAISER:

22 Q. And, I'm sorry, we're adding the
23 attachment to this email as well. It will be --

24 A. Okay.

25 Q. -- Exhibit 22.

1 A. Okay. I got 21.

2 Q. And you see 21 is an email from you to
3 Merritt Beaver?

4 A. Right. I was sensitive to the fact of
5 the -- keeping it very closely held, what the
6 contents of the register are. Right.

7 Q. Right. And -- yeah.

8 So the attachment -- and we'll pull it up
9 in just a second -- is the -- something called the
10 "Remediation Task List."

11 Do you see that?

12 A. Right. It's part of the risk register.
13 It's a tab of an Excel spreadsheet.

14 Q. What is the risk register?

15 A. It's a commonly used practice through
16 security groups, not -- not just Secretary of State,
17 but everywhere, to kind of keep track of all
18 vulnerabilities, whether they are confirmed or not.

19 It's -- it's an ever-growing list of
20 things. You don't delete anything from it because
21 the threat landscape can change and you need to be
22 able to go back and look at things that might have
23 been remediated before on a periodic basis to make
24 sure they're still remediated.

25 So it's just -- you know, it's a list of

Page 174

1 all the things that we need to do.

2 Q. And you said that the remediation task
3 list was just one tab in -- in the Excel spreadsheet
4 that had the whole risk register; is that right?

5 A. Right.

6 Q. And were you responsible for updating that
7 task list?

8 A. Anybody on the security team can add --
9 add, modify, delete -- or not delete, but add or
10 modify. Make up dates, too, as things change.

11 Q. Were -- were you supposed to update that
12 on any regular cadence?

13 A. We usually did it monthly. Or when we got
14 a -- you know, an assessment that came in, like a
15 Fortalice, we'd add to it or we'd go find the same
16 one that was on the list and kind of reprioritize
17 it.

18 I think my role there was just to
19 prioritize the work that was being done and kind of
20 farming it out. As time passed, you know, we'd try
21 to get things done.

22 Q. And it looks like you were being asked to
23 share the risk register with somebody.

24 Do you recall this?

25 A. Let me see -- let me go back to that email

for a second. I want to see if I can recall.

I didn't even give -- I don't think I
shared my risk register with Fortalice. I mean,
it's usually a very closely held -- and I haven't at
any other customer either. I mean, it's not a
Georgia Secretary of State thing. It's a very
defined work list of things and also, to a bad
actor, it would be like a roadmap of how to get in.

23 Q. But you don't recall who asked to take a
24 look --

25 A. I don't.

1 Q. -- at this risk register?

2 A. I don't. I don't know who it would have
3 been.

4 Q. Okay.

5 A. 8/21/20. Was that around the time that we
6 were doing the litigation? I mean, I don't know if
7 that might have been it. Maybe a lawyer asked for
8 it. I'm not sure.

9 I was just concerned of it being public,
10 that's all. Just trying to advise.

11 MS. KAISER: All right. Tab 22, please.

12 (Plaintiffs' Exhibit 23 was marked for
13 identification.)

14 THE WITNESS: So that was 21 and 22. This
15 will be 23?

16 BY MS. KAISER:

17 Q. Oh, apologies. Yep, this will be 23.

18 A. Okay. There it is.

19 Q. Are you familiar with Rule 590-8-3?

20 A. Uh-huh.

21 Q. And just generally, what do you -- what do
22 you recall about that rule, what it requires?

23 A. I think -- I think -- do I put it on here?

24 Q. Yeah. If you -- on page 3, starting --

25 A. Yeah.

Page 177

1 Q. -- on page 3.

2 A. The definitions. I just copied the rule
3 into the document. So...

4 Q. Right. Right.

5 So Section (b), if you look at the middle
6 of the page, says --

7 A. Right.

8 Q. -- "Security of the Voter Registration
9 System is vital to the administration of elections
10 in Georgia. As such, the system shall be maintained
11 in a manner that is consistent with the following
12 security standards."

13 Do you see that?

14 A. Yes, ma'am.

15 Q. And then it lists 27 security standards;
16 right?

17 A. Right.

18 Q. And then Section (c), "Assessments," says,
19 "The Secretary of State shall conduct or have
20 conducted regular cybersecurity assessments of the
21 Voter Registration System."

22 Do you see that?

23 A. I do.

24 Q. And then Subsection (d) essentially
25 requires an annual certification of compliance with

Page 178

1 the rule; is that right?

2 A. Correct.

3 Q. Was it your responsibility to prepare a
4 certification of compliance with Rule 590-8-3?

5 A. Yes. This is my document, so yes.

6 Q. And this is the document for 2020;
7 correct?

8 A. Correct.

9 Q. Did you prepare a certification like this
10 in any other years?

11 A. I think 2020 was the -- the only one I
12 did. I think before that, it was somebody else or
13 it got missed. Again, I don't know. I --

14 Q. On page 6 --

15 A. Okay.

16 Q. -- the second paragraph on page 6, it
17 says, "Currently, our agency does NOT meet the
18 requirements of the rule. Out of the 38
19 requirements we only meet 66%."

20 Do you see that?

21 A. Yes.

22 Q. And so you did an analysis and determined
23 that you only met the -- met the requirements for
24 about two-thirds of the requirements of the rule; is
25 that correct?

Page 179

1 A. Correct. Yeah, it says there if we took
2 the Civix-related ones out, we'd be at 81.

3 Q. And what is Civix?

4 A. The new name for PCC.

5 MS. KAISER: Tab 19, please.

6 (Plaintiffs' Exhibit 24 was marked for
7 identification.)

8 THE WITNESS: Are we done with that one?

9 BY MS. KAISER:

10 Q. Yes. We're adding the next exhibit now,
11 24.

12 Do you have that document in front of you?

13 A. Waiting for it to update.

14 24. Okay. There it is. Okay.

15 Q. All right. This is an email chain from
16 December of 2020.

17 Do you see that?

18 A. Uh-huh.

19 Q. And I'm focused on your email on the --
20 starting on page 1.

21 A. Okay.

22 Q. It looks like you were just sharing some
23 thoughts with folks internal to the Secretary of
24 State's office.

25 Does that look right?

Page 180

1 A. It does.

2 Q. If you look about four paragraphs down, it
3 says, "From a security team perspective, we need
4 more time to focus on the day-to-day operations -
5 all the guys are buried in projects so there is no
6 time to 'watch' or tune things."

7 Do you see that?

8 A. Yeah.

9 Q. What did you mean by this comment?

10 A. As an example, us having to build the
11 servers over at the Election Center and do a bunch
12 of stuff that are usually infrastructure related.
13 That was supposed to be a pretty quick turnaround
14 and just helping out a brother kind of a thing
15 because they were slammed. It ended up being a very
16 long-term project and Michael Barnes didn't want to
17 let go of us. So it -- it became kind of a
18 resource, you know, drain on all of us.

19 I think that's probably one of my -- what
20 I was saying here is we -- we really want to hand
21 this back to the infrastructure team. That's why I
22 copied Bill Warwick and Jason and Kevin. So I think
23 this was my, you know, mea culpa of, "Hey, you know,
24 we've got to address a lot of things and there's
25 just not enough hands." So yeah.

Page 181

1 Q. What effect did it have on the security
2 team's ability to do its work effectively?

3 A. Well, I mean, we had to depend on systems,
4 right, instead of people. And luckily we had very
5 good systems, in that we had, you know, Palo Alto,
6 XDR. We had Cortex on the edge. We had multiple
7 layers of security in some cases, where if one thing
8 broke, then we'd still be okay.

9 But we needed time to continue to tune
10 those as time went on. And the idea there is to
11 reduce the amount of false positives that you get
12 or, even worse, false negatives.

13 So the idea is it's a -- it's a constant
14 thing, you know, to -- to look at this kind of
15 status of everything on a daily basis and make
16 adjustments.

17 And I -- I think my note here was just
18 underlying the fact of, "Hey, infrastructure guys,
19 we really need you to do your -- your part in this
20 so we can get back to our real jobs." So...

21 Q. Are you familiar with a professor at the
22 University of Michigan named Alex Halderman?

23 A. Yes.

24 Q. What do you know about Mr. Halderman?

25 A. He was part of the litigation the last

Page 182

1 time around. He had some specific questions that
2 kind of trickled back towards me. It was -- that
3 was the reason I wrote the second document, to
4 clarify some of the things that he assumed.

5 Q. Did you review any declarations that
6 are -- that were put in by Dr. Halderman?

7 A. At that time I did, yes.

8 Q. Have you reviewed any testimony from
9 Dr. Halderman regarding how easily the BMD system
10 can be hacked?

11 A. No.

12 MR. MILLER: Objection. Lack of
13 foundation.

14 BY MS. KAISER:

15 Q. Were you aware of that testimony?

16 A. In passing, I think. I -- I -- I don't
17 know if my opinion matters when it comes to that.
18 So...

19 It's very easy for an academic to control
20 an environment, given enough time and resources and
21 money, to do anything. So that's where the judgment
22 comes in.

23 So that's what I was trying to get across
24 to the doctor when I responded in that second note,
25 just giving him some clarity about in the

Page 183

1 operational world of running a business, we have to
2 do these things and reprioritize.

3 So that's basically what that was.

4 Q. Do you understand that Dr. Halderman has
5 analyzed the voting equipment that is used in
6 Georgia today to assess the reliability and security
7 of that equipment?

8 A. I didn't know that he personally had done
9 it, no. I know --

10 Q. So you weren't aware that he's issued a
11 detailed report finding that the current system
12 suffers from many significant vulnerabilities?

13 A. I didn't --

14 MR. MILLER: Objection. Lack of
15 foundation.

16 THE WITNESS: Yeah, I -- I didn't. Sorry.
17 BY MS. KAISER:

18 Q. You didn't know -- you just didn't know
19 about that report one way or the other?

20 A. No. I'm not --

21 MR. MILLER: Objection.

22 THE WITNESS: -- in the academic world. I
23 don't spend a lot of time reading papers and
24 things like that. So...

Page 184

1 BY MS. KAISER:

2 Q. I'm sorry. It was not a paper, but a
3 report in this case.

4 A. Yeah, that's fine.

5 MR. MILLER: Objection. Lack of
6 foundation.

7 BY MS. KAISER:

8 Q. So you were not -- not aware of it?

9 MR. MILLER: Same objection.

10 COURT REPORTER: The answer again, please?

11 THE WITNESS: No, I -- I was not aware of
12 it.

13 COURT REPORTER: Thank you.

14 BY MS. KAISER:

15 Q. Do you understand that the current BMD
16 voting system uses QR codes to tally votes?

17 A. I do --

18 MR. MILLER: Objection --

19 THE WITNESS: -- and only because I vote
20 in Georgia. I saw them. So...

21 COURT REPORTER: The objection again,
22 please?

23 MR. MILLER: Lack of foundation.

24 COURT REPORTER: Thank you.

25 Please -- please let him get in an

Page 185

1 objection and her finish the question. Thank
2 you.

3 THE WITNESS: All right.

4 BY MS. KAISER:

5 Q. Are you aware that the current election
6 equipment can be hacked in a way that QR codes can
7 be changed so that they don't reflect what the voter
8 actually intended when they voted on the machine?

9 MR. MILLER: Objection. Lack of
10 foundation.

11 THE WITNESS: I did not.

12 BY MS. KAISER:

13 Q. Based on your experience and training, if
14 that were the case, would you take measures to
15 eliminate that vulnerability?

16 MR. MILLER: Objection. Lack of
17 foundation.

18 THE WITNESS: I don't know if I have
19 enough information, but, yeah, it would
20 definitely go on the list.

21 BY MS. KAISER:

22 Q. Would it be a high priority on the list?

23 MR. MILLER: Same objection.

24 THE WITNESS: I -- again, it -- it all
25 depends on what else was going on at the time.

1 So...

2 BY MS. KAISER:

3 Q. A vulnerability that would allow a QR code
4 to be changed to change votes, would that be
5 considered high priority?

6 MR. MILLER: Objection. Lack of
7 foundation. Asked and answered.

8 THE WITNESS: But the -- the issue is is
9 that -- that system is out of scope for me in
10 my role for Secretary of State. It -- it all
11 belongs to Dominion.

12 So for them, I would imagine it would
13 cause some heartburn, but not -- I -- out of
14 scope for me.

15 BY MS. KAISER:

16 Q. Would it surprise you to learn that the
17 Secretary of State's office has taken no measures to
18 mitigate or eliminate any of the vulnerabilities
19 that Dr. Halderman has found with the existing
20 equipment in Georgia?

21 MR. MILLER: Objection. Lack of
22 foundation. Form of the compound question.
23 Misstates testimony.

24 THE WITNESS: Yeah, I -- I -- I don't know
25 what he -- he brought out. I don't know what

1 his list was.

2 BY MS. KAISER:

3 Q. Based on your experience and training in
4 cybersecurity, if a cybersecurity expert identifies
5 vulnerabilities with a voting system, would you
6 think it would be a high priority to address those
7 vulnerabilities?

8 MR. MILLER: Objection. Lack of
9 foundation. Calls for speculation.

10 THE WITNESS: Yeah, I don't -- I would
11 be -- I'd be suspect of it. Just -- I'd want
12 to look at it myself.

13 BY MS. KAISER:

14 Q. Would you look at it yourself, though?

15 MR. MILLER: Same objection.

16 THE WITNESS: If given the opportunity, I
17 guess, yeah.

18 BY MS. KAISER:

19 Q. And if you, yourself, identified security
20 vulnerabilities, would it be a high priority --
21 priority to fix those vulnerabilities?

22 MR. MILLER: Objection. Lack of
23 foundation. Calls for speculation.

24 THE WITNESS: All depends on the -- the
25 judgment at the time, I guess, of what's going

1 on.

2 BY MS. KAISER:

3 Q. If you had responsibility for voting
4 equipment and you identified a security
5 vulnerability in that equipment, would you consider
6 that an important thing to -- to fix?

7 A. Yes.

8 MR. MILLER: Objection. Lack of
9 foundation. Calls for speculation.

10 THE WITNESS: Sorry.

11 BY MS. KAISER:

12 Q. Your answer was?

13 A. Yes.

14 Q. Thank you.

15 MS. KAISER: All right. Mr. Hamilton, if
16 you'll give us just a minute to confer, I think
17 we're -- we're reaching the end of our
18 questions.

19 THE WITNESS: Okay.

20 MS. KAISER: So we'll go off the record
21 for just a minute, please.

22 VIDEOGRAPHER: The time is 2:15. We're
23 off the record.

24 (Off the record.)

25 VIDEOGRAPHER: The time is 2:27. We're

Page 189

1 back on the record.

2 BY MS. KAISER:

3 Q. Just a few more questions for you,

4 Mr. Hamilton.

5 Q. Are you aware that Dr. -- Dr. Halderman
6 got access to Fulton County's voting equipment in
7 August of 2020?

8 A. No, I didn't.

9 Q. Okay. You were chief information security
10 officer at the time, August 2020; correct?

11 A. Yes.

12 Q. All right. And were you aware that
13 Dr. Halderman testified in an evidentiary hearing in
14 September of 2020 about that election -- about
15 vulnerabilities in that equipment?

16 A. Was that the same one that I did my
17 testifying in or is that a different one?

18 Q. I'm sorry. Did you ever testify at a
19 hearing?

20 A. Yes, ma'am. I was -- I had, like, two
21 questions asked of me, but yeah. It was a
22 federal -- I thought it was the Curling case, the
23 initial part of it, with Judge Totenberg. She asked
24 me to clarify a couple of terms. But --

25 Q. Okay.

Page 190

1 A. -- that was when -- that was when we -- we
2 got Zoom bombed that day. Do you recall that?

3 Q. You know, I wasn't present at the hearing,
4 so I can't recall.

5 A. Okay.

6 MS. KAISER: And, Carey, I'm not sure if
7 you recall either if that was the
8 September 2020 hearing.

9 MR. MILLER: My understanding of the
10 question, I think so, yeah.

11 MS. KAISER: Okay.

12 BY MS. KAISER:

13 Q. Well, so did -- were you present for
14 Dr. Halderman's testimony --

15 A. No.

16 Q. -- in a -- in a hearing?

17 A. No, no, no. I only -- the only people I
18 saw were the ones that were on that day, and he was,
19 I think, on a previous day. That's why I had to
20 respond in writing for his stuff.

21 Q. And are you aware -- are you aware that he
22 testified that he was able to hack the election
23 equipment from Fulton County?

24 MR. MILLER: Objection. Lack of
25 foundation. Calls for speculation.

Page 191

1 THE WITNESS: Yeah, I -- I didn't realize.

2 No, I didn't hear that.

3 BY MS. KAISER:

4 Q. And he was able to do so in just three
5 days?

6 MR. MILLER: Objection. Lack of
7 foundation. Calls for speculation.

8 BY MS. KAISER:

9 Q. You're --

10 A. And this is the --

11 Q. -- not aware of that testimony?

12 A. No. Just as it pertains to that list that
13 I gave.

14 Q. This is not -- this is not about the list
15 of -- from Fortalice; this is --

16 A. Okay.

17 Q. -- this is separate.

18 A. Yeah. I wasn't present for any of that.

19 Q. Okay. And you were not made aware of
20 Dr. Halderman's testimony regarding hacking the
21 actual election equipment from Fulton County?

22 A. No, I was not.

23 MR. MILLER: Objection. Asked and
24 answered.

25 THE WITNESS: Sorry.

Page 192

1 BY MS. KAISER:

2 Q. Would you expect to be made aware of
3 that -- of testimony that the election equipment
4 that Georgia had and was using was able to be hacked
5 in three days?

6 MR. MILLER: Objection. Calls for
7 speculation.

8 THE WITNESS: Yeah, I would think so.

9 BY MS. KAISER:

10 Q. And as -- in your role as chief
11 information security officer for the Secretary of
12 State's office, that's something that you would have
13 liked to know about; is that right?

14 MR. MILLER: Objection. Calls for
15 speculation.

16 COURT REPORTER: The answer again, please?

17 BY MS. KAISER:

18 Q. But nobody told you about that testimony
19 from Dr. Halderman?

20 MR. MILLER: Objection. Lack of
21 foundation. Asked and answered.

22 COURT REPORTER: I didn't hear the
23 previous answer to the question -- the previous
24 question.

25 THE WITNESS: No. "No" was on both.

Page 193

1 Yeah.

2 COURT REPORTER: Thank you.

3 MS. KAISER: I just want to make sure,
4 Ms. Barnes -- I'm sorry, I don't have access to
5 the realtime -- which question did you not have
6 an answer to?

7 COURT REPORTER: One moment, please.

8 (Whereupon, the record was read by the
9 reporter as follows:

10 Question, "In your role as chief
11 information security officer for the Secretary
12 of State's office, that's something that you
13 would have liked to know about; is that
14 right?")

15 THE WITNESS: And I said, yes, that would
16 be nice to know.

17 BY MS. KAISER:

18 Q. Do you have any idea why nobody told you
19 about this testimony from Dr. Halderman?

20 MR. MILLER: Objection. Calls for
21 speculation.

22 THE WITNESS: I don't.

23 BY MS. KAISER:

24 Q. Are you aware of any measures to mitigate
25 the hack that Dr. Halderman executed on the Fulton

1 County election equipment?

2 A. No, I --

3 MR. MILLER: Objection. Lack of
4 foundation. Calls for speculation.

5 THE WITNESS: No, I -- I would expect that
6 to be a Dominion thing. So...

7 BY MS. KAISER:

8 Q. You think -- do you think the Georgia
9 Secretary of State's office would be involved,
10 though?

11 MR. MILLER: Objection. Calls for
12 speculation.

13 THE WITNESS: I -- I would think as a
14 customer, yeah.

15 BY MS. KAISER:

16 Q. And who within the -- the Georgia
17 Secretary of State's office would have
18 responsibility over that?

19 A. Over the machines themselves?

20 Q. Yes, or -- yeah, over identifying or
21 mitigating vulnerabilities with the machines
22 themselves.

23 MR. MILLER: Objection. Lack of
24 foundation.

25 THE WITNESS: Yeah, it was my

Page 195

1 understanding that all of them are actually
2 owned by the individual counties. So --

3 But, yeah, I still think the Secretary of
4 State would want to know that information and
5 then do -- you know, get somebody excited about
6 fixing it if that was the case.

7 BY MS. KAISER:

8 Q. And the person within the Secretary of
9 State's office under whose purview that would fall,
10 don't you think that would be the chief information
11 security officer?

12 MR. MILLER: Objection. Calls for
13 speculation. Lack of foundation.

14 THE WITNESS: I guess if it was in scope,
15 probably, yep.

16 BY MS. KAISER:

17 Q. So this shouldn't just be a Dominion
18 thing, as you said earlier; right? That's something
19 that --

20 A. Well, I mean, it's their -- it's their
21 equipment and it's their code line, so, you know, we
22 can't fix it for them. They would have to do it for
23 us, much like PCC would have to fix their software
24 for us.

25 Q. But the Secretary of State's office would

Page 196

1 have a great interest in making sure that those
2 vulnerabilities were fixed; correct?

3 A. I would think --

4 MR. MILLER: Objection --

5 THE WITNESS: -- so.

6 MR. MILLER: -- asked and answered. Calls
7 for speculation.

8 MS. KAISER: Did you get that answer,
9 Ms. Barnes?

10 COURT REPORTER: I heard, "I would think
11 so."

12 BY MS. KAISER:

13 Q. Are you aware, Mr. Hamilton, that
14 Fortalice conducted an assessment of the BMD
15 equipment in 2019?

16 A. No, actually, not -- you mean the actual
17 polling equipment in the --

18 Q. (Nodded head.)

19 A. No, I didn't realize they did that. That
20 must have been on a -- on a separate statement of
21 work.

22 Q. So you had no involvement with -- with
23 that assessment by Fortalice of the equipment
24 itself?

25 A. No. And it might be just because it was

Page 197

1 excluded from my statement of work from TrustPoint.
2 You know, it was specifically excluded that the
3 actual voting tabulating, Dominion or whatever, was
4 excluded from my responsibilities.

5 MS. KAISER: All right. Just one -- one
6 more minute, Mr. Hamilton. Thank you.

7 THE WITNESS: Okie doke.

8 VIDEOGRAPHER: Would you like to go off
9 the record, Counsel, or stay on?

10 MS. KAISER: [Inaudible], please.

11 VIDEOGRAPHER: I'm sorry. You broke up.

12 MS. KAISER: I said go off the record,
13 please.

14 VIDEOGRAPHER: The time is 2:35. We are
15 off the record.

16 (Off the record.)

17 VIDEOGRAPHER: The time is 2:38. We're
18 back on the record.

19 BY MS. KAISER:

20 Q. Mr. Hamilton, just -- I just want to make
21 sure the record is clear.

22 You're not aware of any request by anyone
23 from the Secretary of State's office to Dominion to
24 fix any of the vulnerabilities that Dr. Halderman
25 identified with the Fulton County voting equipment;

1 is that correct?

2 A. That is --

3 MR. MILLER: Objection --

4 THE WITNESS: -- correct.

5 MR. MILLER: -- lack of foundation.

6 THE WITNESS: I -- I don't recall any
7 conversation specific to Fulton County except
8 for that notebook we talked about.

9 BY MS. KAISER:

10 Q. That was a laptop.

11 A. Laptop, yeah, notebook. Sorry.

12 Q. Right.

13 So with respect to the Fulton County
14 voting equipment that Dr. Halderman tested and was
15 able to hack, you don't recall any instruction to
16 Dominion to fix anything related to that?

17 A. No.

18 MR. MILLER: Objection. Lack of
19 foundation. Asked and answered.

20 THE WITNESS: No.

21 MS. KAISER: All right. No further
22 questions from me, Mr. Hamilton. Thank you
23 very much for your time today.

24 THE WITNESS: Thank you.

25 MR. MILLER: Dave, I'm going to have a

Page 199

1 couple of questions for you. I need to look at
2 my notes real quick.

3 THE WITNESS: Okay.

4 MR. MILLER: I'm sorry to keep going on
5 and off the record, but --

6 THE WITNESS: No, no, that's --

7 MR. MILLER: -- about five minutes.

8 THE WITNESS: -- that's fine.

9 VIDEOGRAPHER: The time is 9- -- I'm
10 sorry, 2:39. We're off the record.

11 (Off the record.)

12 VIDEOGRAPHER: The time is 2:42. We're
13 back on the record.

14 EXAMINATION

15 BY-MR. MILLER:

16 Q. Okay. Mr. Hamilton, I just have a few
17 questions for you before we break here. I'll try
18 and be quick.

19 Ms. Kaiser, at a couple different points,
20 asked you questions including the term "BMD."

21 Do you recall that?

22 A. Yes.

23 Q. Do you understand what "BMD" stands for,
24 the acronym?

25 A. I hadn't heard it until today, but I think

Page 200

1 I've got it correlated now.

2 Q. Okay. And have you ever done any work on
3 BMDs?

4 A. No. I've seen them, you know, as a voter,
5 but...

6 Q. Right.

7 And so as the voter, you have some
8 familiarity with what the BMD is; right?

9 A. Correct.

10 Q. And that would be the touchscreen
11 computer; right?

12 A. Right, iPad or Android, depending on where
13 you go, I guess.

14 Q. And when you vote on those devices, you
15 understand there's a printer connected to that
16 device; right?

17 A. Right, HP printer. I've seen them.

18 Q. And then you understand that that printer
19 prints a ballot to the voter; right?

20 A. Correct.

21 Q. And then as a voter, you then took that
22 ballot to a scanner; right?

23 A. Correct.

24 Q. And so just that I'm -- so that I'm clear,
25 you've -- in your scope of work with the Secretary,

1 you never worked on the ballot-marking devices
2 themselves?

3 A. No, sir, not in any --

4 Q. Never worked on the printer?

5 A. Nope.

6 Q. Never worked on the scanner into which the
7 ballots were fed?

8 A. No, sir.

9 Q. Okay. And was that type of work beyond
10 your work scope?

11 A. It was.

12 Q. So Ms. Kaiser asked you a couple of
13 questions concerning Dr. Halderman.

14 Do you recall that?

15 A. Yes.

16 Q. Are you aware that the report he worked on
17 concerned hacking of that same voting equipment?

18 A. I -- I didn't correlate the two, no.

19 Q. Okay. Knowing that, that would then be
20 outside of your work scope; right?

21 A. Yes.

22 Q. You talked earlier with Ms. Kaiser about
23 the EMS system.

24 Do you recall that?

25 A. Uh-huh.

1 Q. And I'm going to ask you for an audible
2 answer there.

3 A. Yes. I'm sorry.

4 Q. And do you recall discussing with her
5 ballot building or ballot configuration? Do you
6 recall that?

7 A. Yes, sir.

8 Q. And am I correct that you've never done
9 any of that ballot building yourself?

10 A. No, not at any time.

11 Q. Okay. And so when you talked today about
12 your understanding of that process, was that based
13 on an understanding gleaned from others?

14 A. Yes.

15 Q. Ms. Kaiser asked you earlier about a
16 situation in Cobb County.

17 Do you recall what I'm talking about?

18 A. Yes. About the vulnerability, yes.

19 Q. Yeah. Okay.

20 And do you understand what that
21 vulnerability made visible?

22 A. Yes.

23 Q. And what was that?

24 A. Another person's voter registration
25 information.

Page 203

1 Q. Is it your understanding that exploiting
2 that vulnerability would allow you to change a
3 person's voter registration information?

4 A. No. It wasn't an edit screen; it was only
5 a display screen.

6 Q. And I think you had talked with Ms. Kaiser
7 about a similar issue related to MVP.

8 Do you recall that?

9 A. Yes, sir.

10 Q. And in that context, was there any ability
11 to change voter registration information or, like
12 you just mentioned, no -- no editing ability?

13 A. No, it was just the view side. It's
14 displaying your precinct information and things like
15 that.

16 Q. I just want to clarify quickly here.

17 You talked about PCC's services and
18 responsibility related to MVP.

19 Do you recall that?

20 A. I do.

21 Q. And just to make sure I have your
22 testimony correct, it's your testimony today that
23 PCC does not maintain responsibility for the
24 maintenance and operation of MVP; is that accurate?

25 A. Of the hardware and the underlying

Page 204

1 operating system, that is correct. But the
2 application they still have ownership of.

3 Q. And so by that, you mean PCC still writes
4 code to then be used on the hardware; is that
5 accurate?

6 A. Yes, sir.

7 Q. But sitting here today, PCC wouldn't have
8 the ability to -- to access it right now as we speak
9 and -- and adjust something.

10 A. As -- as of the date that I left, we had
11 locked them out of the system and then that --
12 inserted our people into the change control process.

13 So when PCC wanted to change something,
14 then we were party of it, instead of it being kind
15 of a -- a grab bag when they were in charge of it.
16 So it was to formalize the change control.

17 So they -- they still have access to the
18 system when we want them to have it to upload
19 changes, because they change that system a lot, as
20 far as I -- as of the date that I left. I don't --
21 I don't even know if PCC has been released now from
22 State. I don't know if they found another vendor or
23 what the deal is.

24 Q. Okay.

25 A. We didn't talk about that the other day.

1 So...

2 Q. So at the time that your -- you left
3 Secretary of State, do I understand your testimony
4 correctly that -- that PCC on their own could not
5 make a change to MVP?

6 A. Correct.

7 Q. Does that same understanding apply to the
8 ENET system?

9 A. Yes.

10 Q. And just so that I understand the work
11 flow, if a change was needed to be made, am I
12 correct that the Secretary of State would direct PCC
13 to make some change? Is that accurate?

14 A. Correct. Or if -- if they had other
15 changes to go in, they would ask for access. And it
16 was an over-the-shoulder kind of thing, where we
17 would link together in a session and they would do
18 it with us watching the screen.

19 So that was the idea, is to always have
20 kind of a finger on what they were doing so we could
21 have some visibility into what they were doing.

22 So...

23 Q. Okay.

24 A. Without us, they can't get in. So...

25 Q. Okay.

1 MR. MILLER: That's all I have.

2 THE WITNESS: Okay.

3 MS. KAISER: I don't have any further
4 questions. Thank you very much, Mr. Hamilton.

5 THE WITNESS: Oh, you bet. You guys have
6 a great day.

7 VIDEOGRAPHER: This concludes the
8 videotaped deposition. The time is
9 approximately 2:50 p.m. Eastern time. We're
10 off the record.

11 (Deposition concluded at 2:50 p.m.)

12 (Pursuant to Rule 30(e) of the Federal
13 Rules of Civil Procedure and/or O.C.G.A.
14 9-11-30(e), signature of the witness has been
15 reserved.)

16

17

18

19

20

21

22

23

24

25

Page 207

1 C E R T I F I C A T E
2
3

4 STATE OF GEORGIA:
5
6

7 COUNTY OF FULTON:
8
9

10 I hereby certify that the foregoing transcript was
11 taken down, as stated in the caption, and the
12 questions and answers thereto were reduced to
13 typewriting under my direction; that the foregoing
14 pages represent a true, complete, and correct
15 transcript of the evidence given upon said hearing,
16 and I further certify that I am not of kin or
counsel to the parties in the case; am not in the
regular employ of counsel for any of said parties;
nor am I in anywise interested in the result of said
case.

17
18
19
20
21
22
23
24
25
Lee Ann Barnes

LEE ANN BARNES, CCR B-1852, RPR, CRR, CRC

Page 208

1 COURT REPORTER DISCLOSURE
2
3

4 Pursuant to Article 10.B. of the Rules and
5 Regulations of the Board of Court Reporting of the
6 Judicial Council of Georgia which states: "Each
7 court reporter shall tender a disclosure form at the
8 time of the taking of the deposition stating the
9 arrangements made for the reporting services of the
10 certified court reporter, by the certified court
11 reporter, the court reporter's employer, or the
12 referral source for the deposition, with any party
13 to the litigation, counsel to the parties or other
14 entity. Such form shall be attached to the
15 deposition transcript," I make the following
16 disclosure:

17 I am a Georgia Certified Court Reporter. I am here
18 as a representative of Veritext Legal Solutions.
19 Veritext Legal Solutions was contacted to provide
20 court reporting services for the deposition.
21 Veritext Legal Solutions will not be taking this
22 deposition under any contract that is prohibited by
23 O.C.G.A. 9-11-28 (c).

24 Veritext Legal Solutions has no contract/agreement
25 to provide reporting services with any party to the
26 case, any counsel in the case, or any reporter or
27 reporting agency from whom a referral might have
28 been made to cover this deposition. Veritext Legal
29 Solutions will charge its usual and customary rates
30 to all parties in the case, and a financial discount
31 will not be given to any party to this litigation.

32
33 *Lee Ann Barnes*

34 LEE ANN BARNES, CCR B-1852B, RPR, CRR, CRC
35
36

Page 209

1 To: CAREY MILLER, ESQ.
2 Re: Signature of Deponent David Hamilton
3 Date Errata due back at our offices:
4

5 Greetings:

6 This deposition has been requested for read and sign
7 by the deponent. It is the deponent's
responsibility to review the transcript, noting any
changes or corrections on the attached PDF Errata.
8 The deponent may fill out the Errata electronically
or print and fill out manually.

9
10 Once the Errata is signed by the deponent and
11 notarized, please mail it to the offices of Veritext
(below).

12 When the signed Errata is returned to us, we will
13 seal and forward to the taking attorney to file with
the original transcript. We will also send copies
of the Errata to all ordering parties.

14
15 If the signed Errata is not returned within the time
above, the original transcript may be filed with the
16 court without the signature of the deponent.

17
18 Please send completed Errata to:
19 Veritext Production Facility
20 20 Mansell Court, Suite 300
21 Roswell, GA 30076
22 (770) 343-9696

23
24 5036176
25

Page 210

1 ERRATA for ASSIGNMENT #5036176
2 I, the undersigned, do hereby certify that I have
3 read the transcript of my testimony, and that
4 ____ There are no changes noted.
5 ____ The following changes are noted:
6
7 Pursuant to Rule 30(7)(e) of the Federal Rules of
8 Civil Procedure and/or OCGA 9-11-30(e), any changes
9 in form or substance which you desire to make to
10 your testimony shall be entered upon the deposition
11 with a statement of the reasons given for making
12 them. To assist you in making any such corrections,
13 please use the form below. If additional pages are
14 necessary, please furnish same and attach.
15 Page ____ Line ____ Change to: _____
16 Reason for change: _____
17 Page ____ Line ____ Change to: _____
18 Reason for change: _____
19 Page ____ Line ____ Change to: _____
20 Reason for change: _____
21 Page ____ Line ____ Change to: _____
22 Reason for change: _____
23 Page ____ Line ____ Change to: _____
24 Reason for change: _____
25 5036176

Page 211

1 Page ____ Line ____ Change to: _____

2 Reason for change: _____

3 Page ____ Line ____ Change to: _____

4 Reason for change: _____

5 Page ____ Line ____ Change to: _____

6 Reason for change: _____

7 Page ____ Line ____ Change to: _____

8 Reason for change: _____

9 Page ____ Line ____ Change to: _____

10 Reason for change: _____

11 Page ____ Line ____ Change to: _____

12 Reason for change: _____

13 Page ____ Line ____ Change to: _____

14 Reason for change: _____

15 Page ____ Line ____ Change to: _____

16 Reason for change: _____

17 Page ____ Line ____ Change to: _____

18 Reason for change: _____

19 DEPONENT'S SIGNATURE
20 Sworn to and subscribed before me this _____ day

21 of _____, 20__.
22 _____
23 Notary Public

24 My commission expires _____
25 5036176